Google Inc. et al v. Egger et al Doc. 481

CINDY COHN (CSB No. 145997)
cindy@eff.org
LEE TIEN (CSB No. 148216)
KURT OPSAHL (CSB No. 191303)
KEVIN S. BANKSTON (CSB No. 217026)
CORYNNE MCSHERRY (CSB No. 221504)
JAMES S. TYRE (CSB No. 83117)
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Counsel For AT&T Class Plaintiffs And
Co-Lead Coordinating Counsel

RICHARD R. WIEBE (CSB No. 121156)
LAW OFFICE OF RICHARD R. WIEBE
425 California Street, Suite 2025
San Francisco, CA 94104
Telephone: (415) 433-3200
Facsimile: (415) 433-6382

ARAM ANTARAMIAN
LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
Berkeley, CA 94703
Telephone: (510) 841-2369

Counsel For AT&T Class Plaintiffs
[Additional Counsel On Signature Page]

HARVEY GROSSMAN
ADAM SCHWARTZ
ROGER BALDWIN FOUNDATION OF ACLU
180 North Michigan Avenue
Suite 2300
Chicago, IL 60601
Telephone: (312) 201-9740
Facsimile: (312) 201-9760

Counsel For AT&T Class Plaintiffs And
Co-Lead Coordinating Counsel

[Additional Counsel On Last Page]

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION, MDL No. 1791

This Document Relates To All Cases Except: *Al-Haramain Islamic Foundation, Inc. v. Bush*, No. 07-0109; *Center for Constitutional Rights v. Bush*, No. 07-1115; *Guzzi v. Bush*, No. 06-06225; *Shubert v. Bush*, No. 07-0693; *Clayton v. AT&T Commc'ns of the Southwest*, No. 07-1187; *U. S. v. Adams*, No. 07-1323; *U. S. v. Clayton*, No. 07-1242; *U. S. v. Palermino*, No. 07-1326; *U. S. v. Rabner*, No. 07-1324; *U. S. v. Volz*, No. 07-1396

MDL Docket No 06-1791 VRW

PLAINTIFFS' FEDERAL RULE OF EVIDENCE SECTION 1006 SUMMARY OF VOLUMINOUS EVIDENCE FILED IN SUPPORT OF PLAINTIFFS' OPPOSITION TO MOTION OF THE UNITED STATES SEEKING TO APPLY FISAAA § 802 (50 U.S.C. § 1885a) TO DISMISS THESE ACTIONS

Date: December 2, 2008
Time: 10:00 a.m.
Courtroom: 6, 17th Floor
Judge: The Hon. Vaughn R. Walker

Dockets.Justia.com

TABLE OF CONTENTS

INTRODUCTION 1

SUMMARY OF VOLUMINOUS WRITINGS PURSUANT TO FEDERAL RULE OF EVIDENCE 1006 6

I. OVERVIEW OF THE PROGRAM 6

A. EVIDENCE SHOWING THE PROGRAM ORIGINATED OUTSIDE OF FISA 7

B. EVIDENCE SHOWING HOW THE PROGRAM OPERATES 11

1. Wholesale acquisition of communications (including content and non-content). 11

2. Automated analysis, or datamining, of content and non-content information. 14

3. No minimization before acquisition, storage, data mining, or analysis by a human agent and inadequate minimization thereafter. 18

II. EVIDENCE OF THE TELECOMMUNICATIONS CARRIERS' COLLABORATION WITH THE GOVERNMENT PROGRAM 21

A. EVIDENCE OF COMMUNICATIONS SURVEILLANCE 25

B. EVIDENCE OF CALL RECORDS SURVEILLANCE 26

C. EVIDENCE THAT AT&T PARTICIPATED IN THE PROGRAM 33

1. Evidence of AT&T's collaboration with the communications acquisition aspect of the Program 33

2. Evidence of AT&T's collaboration with the call detail records aspect of the Program 38

D. EVIDENCE THAT VERIZON PARTICIPATED IN THE PROGRAM 38

III. THE EVOLUTION OF THE PROGRAM OVER TIME 41

A. MARCH 2004 ADMINISTRATION REVOLT OVER ILLEGAL SURVEILLANCE 41

B. 2007 INTERACTIONS WITH FISA COURT 46

C. THE PROGRAM AFTER THE PROTECT AMERICA ACT OF 2007 49

IV. EVIDENCE PROVIDING CONTEXT FOR GOVERNMENT ASSERTIONS ON THE PROGRAM 50

A. THERE IS NO SEPARATE TERRORIST SURVEILLANCE PROGRAM 50

B. SURVEILLANCE THAT IS LATER MINIMIZED IS STILL SURVEILLANCE 53

C. MISLEADING USE OF THE TERMS "CONTENT," "COMMUNICATIONS" AND "CONVERSATIONS". 54

D. THE GOVERNMENT'S ASSERTIONS OF HARM TO NATIONAL SECURITY ARE NOT CREDIBLE. 56

V. EVIDENCE OF ATTORNEY GENERAL MUKASEY'S BIAS ON TELECOM IMMUNITY 58

A. EVIDENCE OF THE ATTORNEY GENERAL'S INSTITUTIONAL RESPONSIBILITIES THAT PROVIDE A STRONG MOTIVE TO RULE IN A WAY THAT WOULD AID THE INSTITUTION 58

B. EVIDENCE THAT THE ATTORNEY GENERAL HAS PREJUDGED THIS MATTER 59

CONCLUSION 61

INTRODUCTION

Plaintiffs submit this Summary of Voluminous Evidence pursuant to Federal Rule of Evidence 1006 to assist the Court in its assessment of whether or not there is substantial evidence supporting the Public Certification of the Attorney General of the United States (Case M:06-cv-01791-VRW ("MDL") Dkt. 469-3) ("Mukasey Certification") that the telecom defendants are entitled to dismissal of these actions under Section 802. The evidence contained in this voluminous record supports plaintiffs' Opposition To Motion Of The United States Seeking To Apply FISAAA Section 802 (50 U.S.C. § 1885a) To Dismiss These Actions ("Section 802 Opposition"). Because the record is so large, and because new relevant public domain information continues to come to light, a Summary of Voluminous Evidence is an appropriate submission to assist the Court. *See* Fed. R. Evid. 1006 ("The contents of voluminous writings, recordings, or photographs which cannot conveniently be examined in court may be presented in the form of a chart, summary, or calculation.")

As this Court is aware, plaintiffs' allegations primarily challenge two practices: the dragnet acquisition of the communications of millions of Americans, including the named plaintiffs and the class members, and the disclosure to the government of the communications records of millions of Americans, including the named plaintiffs and the class members. *See, e.g., Hepting v. AT&T Corp.*, 439 F.Supp.2d 974, 978 (N.D. Cal. 2006) (listing statutory and constitutional causes of action in *Hepting* lawsuit). The dragnet allegations focus on "acquisition by an electronic, mechanical, or other surveillance device," such as the fiber-optic splitters in AT&T's Folsom Street facility and other facilities that are at the heart of the lawsuits against AT&T, which involve the acquisition of both content and non-content information. The communications records allegations focus on the telecommunications companies' disclosure of call-detail records to the government. Collectively the warrantless domestic surveillance program involving the dragnet acquisition of communications (including both content and non-content information) by surveillance devices, as well as the disclosure of communications records constitutes the "Program."

This Summary of Voluminous Evidence compiles in one document with supporting exhibits the evidence demonstrating that the defendant telecommunications companies participated in the Program and that their participation does not fall under any of the provisions of section 802(a) of the FISA Amendments Act of 2008.[1]

Section I summarizes the evidence establishing the existence of the Program. The Program involves a content-dragnet, where the entirety of communications transiting over domestic telecommunications facilities is diverted to the government and placed into National Security Agency ("NSA") databases, as well as the disclosure and analysis of communications records, such as call-detail records. After the communications are acquired (with the assistance of the telecommunications companies), the government uses sophisticated computers to analyze the accumulated meta-data, including content of communications such as email subject lines, online addresses ("URLs") and online search terms, to determine which communications to subject to further analysis. Moreover, the evidence shows that the government knew the Program violated statutes like the Foreign Intelligence Surveillance Act of 1978 ("FISA"), 50 U.S.C. §§ 1801 *et seq*., the statute regulating electronic surveillance for foreign intelligence purposes.

Section II summarizes the evidence showing that the defendant carriers provided (or provided access to) information (including communication contents, communications records, or other information relating to a customer or communication), as well as access to their telecommunications facilities. To assist in the Program, the defendant carriers provided the entire communication stream (*e.g.,* by a fiber-optic splitter), as well as disclosing their existing databases of communications records. Section II summarizes the evidence about the defendant carriers' role overall, as well as specific evidence regarding the roles of particular defendants.

Section III summarizes significant events in the Program over time, including the March 2004 disputes over the legality of the Program that nearly led to the resignation of two dozen senior government officials, the interactions with the Foreign Intelligence Surveillance Court ("FISC") in January 2007, the passage of the Protect America Act of 2007 ("PAA"), and the Program today.

[1] Copies of the evidence summarized here have been manually filed with the Court and served on the government and the telecommunications defendants.

The evidence summarized in section IV provides the Court with critical context to assist in evaluating the government's non-public certifications about the Program. This Section includes the evidence regarding the government's use of key terms, like the so-called "Terrorist Surveillance Program," "surveillance" and "content." For example, despite the government's continued use of the term, the evidence shows that there is not, and never has been, a separate, narrowly circumscribed Terrorist Surveillance Program. Section IV also summarizes the facts casting doubt on the credibility of the governments' assertions that grave danger would result from the revelation or confirmation of *any* information about the defendant carriers' participation in the Program.

Section V summarizes the evidence showing that Attorney General Michael Mukasey is not an impartial fact-finder and has prejudged whether or not the carriers should get immunity.

The Summary of Voluminous Evidence is based on documents filed in the various cases in this Multi-District Litigation; admissions in government documents; publicly reported admissions by the government; statements by the defendants, the Administration and Members of Congress; transcripts of relevant press conferences and congressional hearings; and the statements and declarations of third-party witnesses, including the declarations of Mark Klein and J. Scott Marcus in the *Hepting* action.

We offer this Summary for the convenience of the Court. The evidence in support of plaintiffs' Section 802 Opposition is, quite simply, voluminous. The government's Motion Of The United States Seeking To Apply FISAAA Section 802 (50 U.S.C. § 1885a) To Dismiss These Actions (MDL Dkt. No. 469) ("Section 802 Motion") raises many different factual and legal issues, and plaintiffs collect and summarize all of the counter-evidence here. "Rule 1006 does not require that 'it be literally impossible to examine the underlying records.'" *U.S. v. Stephens*, 779 F.2d 232, 238-39 (5th Cir. 1985) (quoting *U.S. v. Scales*, 594 F.2d 558, 562 (6th Cir. 1978), *cert. denied*, 441 U.S. 946 (1979)). "The fact that the underlying documents are already in evidence does not mean that they can be 'conveniently examined in court.' " *Stephens*, 779 F.2d at 239 (quoting *U.S. v. Lemire*, 720 F.2d 1327, 1347 (D.C. Cir. 1983)).

This Court may rely on the evidence contained in this Summary of Voluminous Evidence for the purposes of determining whether to grant or deny the pending motion. This Summary of Voluminous Evidence includes many documents that are already in the record in a number of different actions that are a part of this MDL proceeding, as well as new evidence. Rule 1006 requires that the summary document be based on foundation testimony connecting it with underlying evidence summarized, and must fairly represent competent evidence already before the trier of fact. *Fagiola v. Nat'l Gypsum Co. AC & S., Inc.*, 906 F.2d 53, 57 (2d Cir. 1990) ("Evidence admitted under Rule 1006 must be otherwise admissible and remains subject to the usual objections under the rules of evidence and the Constitution.") *see also U.S. v. Milkiewicz*, 470 F.3d 390, 396 (1st Cir. 2006). However, at the summary judgment stage, in examining the evidence of a party *opposing* summary judgment, courts do not focus on the admissibility of the evidence's form, but rather on the potential admissibility at trial of its contents. *Fraser v. Goodale*, 342 F.3d 1032, 1036-37 (9th Cir. 2003) (citing *Block v. City of Los Angeles*, 253 F.3d 410, 418-19 (9th Cir. 2001) ("To survive summary judgment, a party does not necessarily have to produce evidence in a form that would be admissible at trial, as long as the party satisfies the requirements of Federal Rules of Civil Procedure 56."); *Fed. Deposit Ins. Corp. v. N.H. Ins. Co.*, 953 F.2d 478, 485 (9th Cir. 1991) ("the nonmoving party need not produce evidence in a form that would be admissible at trial in order to avoid summary judgment.") (internal quotation marks and citation omitted). For example, even if a statement quoted in a book or a newspaper article is hearsay, the information asserted in such an article would be admissible in a subsequent trial through the testimony of the person quoted, or by establishing the foundation for a hearsay exception or that the statement was a non-hearsay admission. Moreover, at this stage in the litigation, the Court is entitled to use circumstantial evidence and to draw inferences there from. *In re Sealed Case*, 494 F.3d 139, 147 (D.C. Cir. 2007). Accordingly, for purposes of this motion, the Court may consider all of the evidence contained in this Summary of Voluminous Evidence.

In preparing and presenting this Summary, plaintiffs have complied with Rule 1006: the evidence upon which the Summary is based is available for inspection, such evidence has been authenticated, and this Summary is based on that authenticated evidence. *See* Declaration of Kurt

Opsahl Regarding Plaintiff's Evidence Rule 1006 Summary of Voluminous Evidence Filed in Support of Plaintiffs' Opposition To Motion Of The United States Seeking To Apply FISAAA § 802 (50 U.S.C. § 1885A) To Dismiss These Actions ("Opsahl Decl.") at ¶¶ 2, 4-82. Accordingly, the Court may rely on this Summary.

SUMMARY OF VOLUMINOUS WRITINGS PURSUANT TO FEDERAL RULE OF EVIDENCE 1006

I. Overview of The Program

Shortly after the September 11, 2001 terrorist attacks, President George W. Bush authorized the NSA to conduct warrantless surveillance of telephone and Internet communications of persons within the United States. March 31, 2006 Request for Judicial Notice (Case No. 3:06-cv-00672-VRW ("Hepting") Dkt. 20-1) ("March 2006 RJN") at ¶¶ 1, 2 [Vol. V, Ex. 77, p. 1772].[2] (Please note that evidence in the docket summarized here has been refiled for the Court's convenience in attached volumes of Evidence In Support of Plaintiffs' Opposition (hereinafter cited by volume, exhibit and page number.))

On October 4, 2001, the President issued a secret presidential order ("Program Order") that "authorized the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying." Mar. 31, 2006 Declaration of Cindy Cohn (Hepting Dkt. 19) ("Cohn Decl."), Ex. J [Vol. V, Ex. 76, p. 1764] (James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005)); Opsahl Decl. Ex. 1, [Vol. I, p. 1] (ERIC LICHTBLAU, BUSH'S LAW: THE REMAKING OF AMERICAN JUSTICE 157 (Pantheon Books 2008) ("BUSH'S LAW")).[3] (New evidence summarized here is described in the Opsahl Declaration and filed for the Court's convenience in the volumes of Evidence In Support of Plaintiffs' Opposition (hereinafter cited by volume and page number.)

The Program of NSA surveillance inside the United States began on October 6, 2001.[4] Opsahl Decl. Ex. 2, [Vol. I, p. 65] (Hearing of the S. Select Comm. on Intelligence on the

[2] S*ee also* Cohn Decl. Exs. C and J [Vol. V, Ex. 76, pp. 1714, 01764] (James Risen & Eric Lichtblau, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. TIMES (Dec. 24, 2005), and James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005)); Declaration of Lt. Gen. Keith B. Alexander (MDL Dkt. 254-4) at ¶ 10 [Vol. VI, Ex. 84, p. 2539].

[3] *See also* S. Rep. 110–209 (MDL Dkt. 469-2) at 5 [Vol. VIII, Ex. 90, p. 3034].

[4] Prior to the official inception of the Program, "[w]ithin hours and days of the attacks, the NSA began ratcheting up its unmatched spyware, with the help of the U.S. telecom giants, to pore through vast amounts of communications flowing into and out of Afghanistan." BUSH'S LAW, at 142 [Vol. I, Ex. 1].

Nomination of Gen. Michael V. Hayden to be the Dir. of the Central Intelligence Agency, 109th Cong. 62 (May 18, 2006) ("Hayden Hearing")). The President renewed his October 4, 2001 order at least 30 times, approximately every 45 days. March 2006 RJN, at ¶ 3 [Vol. V, Ex. 77, p. 1773]. In response to a June 27, 2007 subpoena[5] issued by the Committee on the Judiciary to the Office of the Vice President relating to past warrantless electronic surveillance, the Office of the Vice President identified 43 Program Orders (and two amended Program Orders) (identified as Top Secret/Codeword Presidential Authorizations) between October 4, 2001 and December 2006.[6] Opsahl Decl. Ex. 3 [Vol. I, p. 177] (Letter from Shannen W. Coffin, Counsel to the Vice President, Office of the Vice President, to Sen. Patrick J. Leahy, Chairman, S. Comm. on the Judiciary, and Sen. Arlen Specter, Ranking Minority Member, S. Comm. on the Judiciary (Aug. 20, 2007) ("OVP Subpoena Response")).

A. Evidence Showing the Program Originated Outside of FISA

The Program reflects a goal of the NSA presented to the incoming Bush administration in December 2000. "The volumes and routing of data make finding and processing nuggets of intelligence information more difficult. To perform both its offensive and defensive mission, NSA must 'live on the network.'" Opsahl Decl. Ex. 4 [Vol. I, p. 214] (National Security Agency, *Transition 2001* (December 2000), at 31). Moreover, the NSA asserted that its "mission will demand a powerful, permanent presence on a global telecommunications network that will host the 'protected' communications of Americans as well as the targeted communications of adversaries." *Id*. at 32 [Vol. I, p. 215].

---

[5] *Available at* http://media.washingtonpost.com/wp-srv/politics/documents/senate_judiciary_subpoena_to_cheney_26.pdf.

[6] The identified dates were October 4, November 2, and November 30, 2001; January 9, March 14, April 18, May 21, June 24, July 30, September 10, October 15, and November 18, 2002; January 8, February 7, March 17, April 22, June 11, July 14, September 10, October 15 and December 9, 2003; January 14, March 11 (including as amended by the Presidential Memoranda of March 19 and April 2), May 5, June 23, August 9, September 17, and November 17, 2004; January 11, March 1, April 19, June 14, July 26, September 10, October 26, and December 13, 2005; and January 27, March 21, May 16, July 6, September 6, October 24, and December 8, 2006.

The Program meets that goal. As Rep. Silvestre Reyes, Chairman of the House Permanent Select Committee On Intelligence (who has been briefed on the Program),[7] explained at a September 2007 hearing, "[t]he NSA program involved not only targets overseas, but also American citizens whose phone calls were listened to and e-mail read without a warrant." Opsahl Decl. Ex. 5 [Vol. I, p. 223] *FISA Hearing:* Hearing Before the H. Permanent Select Comm. on Intelligence, 110th Cong. 2 (Sept. 18, 2007) (statement of Rep. Silvestre Reyes, Chairman, H. Permanent Select Comm. on Intelligence); Opsahl Decl. Ex. 8 [Vol. I, p. 385] BARTON GELLMAN, ANGLER: THE CHENEY VICE PRESIDENCY 145 (Penguin Press 2008) ("ANGLER") ("The U.S. government was sweeping in e-mails, faxes, and telephone calls of its own citizens, in their own country. Transactional data, such as telephone logs and e-mail headers, were collected by the billions.")

While President Bush ultimately signed the Program Order initiating the Program, Vice President Cheney and the legal counsel to the Office of the Vice President, David Addington, "guided the program's expansion and development … it was Addington who wrote [the Program Orders], defining the reach of warrantless intrusion into the lives of Americans." ANGLER, at 282 [Vol. I, Ex. 8]; *see also* BUSH'S LAW at 144-147 [Vol. I, Ex. 1] (discussing origins of the Program). Addington "was the chief legal architect of the Terrorist Surveillance Program … He and the vice president had abhorred FISA's intrusion on presidential power ever since its enactment in 1978.

---

[7] Opsahl Decl. Ex. 5 [Vol. I, p. 224] (*The Foreign Intelligence Surveillance Act*: Hearing before the H. Permanent Select Comm. on Intelligence 3 (Sept. 18, 2007) (Chairman Reyes: "We have held four hearings in June and July. Committee members and staff have made several trips to NSA to review this new authority [the Protect America Act]. We have held a closed hearing on September the 6th with the NSA and FBI directors…")); *Id.* Ex. 6 [Vol. I, p. 346 (Dept. of Justice Press Release, *Transcript Of Background Briefing on FISA Authority Of Electronic Surveillance By Senior Justice Department Officials On FISA Authority Of Electronic Surveillance* (Jan. 17, 2007), at 4 (As of January 2007, "the full Intelligence committees, both in the Senate and the House, are fully briefed . . .). "The process of being 'read in' to a compartmented program generally entails receiving a briefing about the program followed by a formal acknowledgement of the briefing, usually indicated by the signing of a non-disclosure agreement binding the individual to obligations regarding the handling and use of information concerning the program." *Id.* Ex. 7 [Vol. I, p. 363 (Office of the Inspector Gen., U.S. Dept. of Justice, *Report of Investigation Regarding Allegations of Mishandling of Classified Documents by Att'y Gen. Alberto Gonzales* (Sept. 2, 2008) ("OIG Gonzales Report") at 8, n.10.)

After 9/11 they and other top officials in the administration dealt with FISA the way they dealt with other laws they didn't like: They blew through them in secret based on flimsy legal opinions that they guarded closely so no one could question the legal basis for the operations." Opsahl Decl. Ex. 9 [Vol. I] JACK L. GOLDSMITH,[8] THE TERROR PRESIDENCY: LAW AND JUDGMENT INSIDE THE BUSH ADMINISTRATION 181 (W. W. Norton 2007) ("THE TERROR PRESIDENCY").

Addington and then White House Counsel Alberto Gonzales assigned John Yoo, then a Deputy Assistant Attorney General in the Office of Legal Counsel, to prepare the Program's legal opinions. BUSH'S LAW, at 156 [Vol. I, Ex. 1]; ANGLER at 283 [Vol. I, Ex. 8]. The Department of Justice prepared memoranda dated October 4 and November 2, 2001; January 9, May 17, and October 11, 2002; February 25, 2003; March 15, May 6, and July 16, 2004; and February 4, 2005. OVP Subpoena Response, *supra* [Vol. I, p. 177]. Years later, after he left government service in 2003, Yoo explained why FISA was not sufficient for the Program's dragnet interception:

> [U]nder existing laws like FISA, you have to have the name of somebody, have to already suspect that someone's a terrorist before you can get a warrant. You have to have a name to put in the warrant to tap their phone calls, and so it doesn't allow you as a government to use judgment based on probability to say: "Well, 1 percent probability of the calls from or maybe 50 percent of the calls are coming out of this one city in Afghanistan, and there's a high probability that some of those calls are terrorist communications. But we don't know the names of the people making those calls." You want to get at those phone calls, those e-mails, but under FISA you can't do that.

Opsahl Decl. Ex. 10 [Vol. I, p. 394] Interview by PBS Frontline with John C. Yoo (Jan. 10, 2007).[9]

---

[8] Goldsmith was the Assistant Attorney General for the Office of Legal Counsel in the Department of Justice from October 2003 to July 2004.

[9] S*ee also* BUSH'S LAW, at 143-44 [Vol. I, Ex. 1] (discussing reasons for evading FISA); Cohn Decl. Ex. G [Vol. V, Ex. 76, p. 1753] ((Morton Kondracke, *NSA Data Mining is Legal, Necessary, Chertoff Says,* ROLL CALL, (Jan. 19, 2006) (Homeland Security Secretary Chertoff "said that getting an ordinary FISA warrant is 'a voluminous, time-consuming process' and 'if you're culling through literally thousands of phone numbers ... you could wind up with a huge problem managing the amount of paper you'd have to generate.'")); Opsahl Decl. Ex. 93 [Vol. VII] (JAMES RISEN, STATE OF WAR: THE SECRET HISTORY OF THE CIA AND THE BUSH ADMINISTRATION 48 (Simon & Schuster 2006) ("administration officials say that one reason they decided not to seek court-approved search warrants for the NSA operation was that the volume of telephone calls and e-mails being monitored was so big that it would be impossible to get speedy court approval for all of them.")); *Id.* Ex. 11 [Vol. II, p. 444] (*Dept. of Justice Oversight*: Hearing before the S. Comm. on the Judiciary 110th Cong. 41 (Jan. 18, 2007) ("Jan. 18, 2007 Gonzales Testimony")) (testimony of Alberto Gonzales, Att'y Gen. of the U.S.: "the administration started down this road just months

The government has candidly admitted that FISA "requires a court order before engaging in this kind of surveillance . . . unless otherwise authorized by statute or by Congress." March 2006 RJN at ¶ 4 [Vol. V, Ex. 77, p. 1773]. The Program admittedly operated "in lieu of" court orders or other judicial authorization, *Id.* at ¶¶ 6-7 [Vol. V, Ex. 77, p. 1774-75], and neither the President nor Attorney General authorizes the specific interceptions. *Id.* at ¶ 9 [Vol. V, Ex. 77, p. 1175]; *see also* Opsahl Decl. Ex. 12 [Vol. II, p. 696] (*Proposed FISA Modernization Legislation*: Hearing before the S. Select Comm. on Intelligence, 110th Cong. 36 (May 1, 2007)) (Testimony of Benjamin Powell, General Counsel, Office of the Dir. of Nat'l Intelligence, that surveillance that was "done under the president's authorization and the president's authority were not done pursuant to FISA or attorney general emergency authorizations by which after 72 hours you would go to the FISA Court."). As General (Ret.) Michael V. Hayden, the former Principal Deputy Director for National Intelligence, put it, the Program "is a more . . . 'aggressive' program than would be traditionally available under FISA," in part because "[t]he trigger is quicker and a bit softer than it is for a FISA warrant." March 2006 RJN at ¶ 10 [Vol. V, Ex. 77, p. 1777]; *see also* Opsahl Decl. Ex. 11 [Vol. II, p. 444] (*Dept. of Justice Oversight*: Hearing before the S. Comm. on the Judiciary, 110th Cong. 12 (Jan. 18, 2007) ("Jan. 18, 2007 Gonzales Testimony") (Testimony of Alberto Gonzales, Att'y Gen. of the U.S.: "we looked at FISA and we all concluded, there is no way we can do what we believe we have to do to protect this country under the strict reading of FISA.")); Opsahl Decl. Ex. 92 [Vol. VII, p. 3213] (*The Foreign Intelligence Surveillance Act*: Hearing before the H. Permanent Select Comm. on Intelligence, 110th Cong. 84 (Sept. 20, 2007) (Testimony of J. Michael McConnell, Dir. of Nat'l Intelligence, that "the original program that the President was operating" was unlawful in the "framework of FISA," while reserving judgment on the Article II argument)). The only review process is authorization by an NSA "shift supervisor" for direct review of particular individuals' communication. March 2006 RJN at ¶¶ 6, 9 [Vol. V, Ex. 77, p. 1776]; *see also* Opsahl Decl. Ex. 13 [Vol. II, p. 706] (*The Terrorist Surveillance Program and the Foreign Intelligence Surveillance Act (FISA)*: Hearing of the Subcomm. on the Constitution, Civil Rights,

---

after the attacks of September 11th because we did not believe that FISA was available to allow the United States to engage in this kind of foreign collection…").

and Civil Liberties, H. Comm. on the Judiciary, 110th Cong. 2 (June 7, 2007)) (Statement of Steven G. Bradbury, Principal Deputy Asst. Att'y Gen., Office of Legal Counsel, U.S. Dept. of Justice: "Highly trained intelligence professionals made the initial decision to target communications for interception.")

B. Evidence Showing How the Program Operates

1. Wholesale acquisition of communications (including content and non-content).

The government conducts surveillance under the Program in several stages, starting with acquisition of the all the communications passing through telecommunications switches. As part of the Program "[telecommunications] companies have granted the NSA access to their all-important switches, the hubs through which colossal volumes of voice calls and data transmissions move every second…. [T]he NSA appears to be vacuuming up all data, generally without a particular phone line, name, or e-mail address as a target." Cohn Decl. Ex. D [Vol. V, Ex. 76, p. 1718-19] (Shane Harris & Tim Naftali, *Tinker, Tailor, Miner, Spy: Why the NSA's Snooping Is Unprecedented In Scale and Scope*, SLATE (Jan. 3, 2006)).

Plaintiffs' evidence establishing AT&T's participation in the Program illustrates that Program surveillance starts with wholesale acquisition of communications content. In January 2006, a former AT&T employee named Mark Klein provided detailed eyewitness testimony and documentary evidence showing how the telecom defendants, and AT&T in particular, are acquiring communications for the government. Klein had worked as an AT&T technician for 22 years, most recently at AT&T's San Francisco facility on Folsom Street. Declaration of Mark Klein (Hepting Dkt. 31 [Vol. V, Ex. 78, p. 2041]) ("Klein Decl.").[10]

[10] Klein is a former AT&T Corp. employee who retired in May 2004. Klein Decl. ¶¶ 2-6 [Vol. V, Ex. 78, p. 2041]. During his 22 years of employment at AT&T Corp., he worked as a communications technician and as a computer network associate at various locations. *Id.* ¶¶ 2-5 [*Id.*]. In the period relevant to this motion, he worked at a facility that handled AT&T's WorldNet International Service ("Geary Facility"), *id.* ¶¶ 8-9 [Vol. V, Ex. 78, p. 2042], and at the Folsom Street Facility which handled AT&T's WorldNet International Service, such as dial-up and DSL Internet service. *Id.* ¶¶ 15, 19 [Vol. V, Ex. 78, p. 2042-43].

As Klein's documents show, Internet communications are carried as light signals on fiber-optic cables. *Id.* ¶¶ 21-24; *See also* Declaration of J. Scott Marcus. (Hepting Dkt. 32) at ¶ 52 [Vol. VI, Ex. 79, p. 2091] ("Marcus Decl."). To divert the communications, AT&T connected the fiber-optic cables entering its WorldNet Internet room to a "splitter cabinet." Klein Decl. at ¶¶ 25-34 [Vol. V, Ex. 78, p. 2044-45]. The splitter cabinet split the light signals from the WorldNet Internet service in two, making two identical copies of the material carried on the light signal. *Id.* The splitter cabinet directed one portion of the light signal through fiber optic cables into a secret room built on AT&T premises, but controlled by the NSA while allowing the other portion to travel its normal course to its intended destination. *Id.* ¶¶ 27-34 [*Id.*]. The split cables carried domestic and international communications of AT&T customers, as well as communications from users of other non-AT&T networks that pass through the Folsom Street Facility. *Id.* ¶¶ 31-34 [Vol. V, Ex. 78, p. 2045].

Plaintiffs retained an expert in information technology and telecommunications to explain the implications of the documents and testimony Klein furnished. *See* Marcus Decl. and Exhibits [Vol. VI, Ex. 79, p. 2077-2446]. The expert, J. Scott Marcus, spent decades working for a variety of telecommunications clients, including AT&T, and served as a senior technical advisor for Internet technology to the Federal Communications Commission ("FCC") from July 2001 until July 2005 and as a member of the FCC's Homeland Security Policy Council.

In particular, Marcus illustrates that the position or location of the fiber split in the Surveillance Configuration was not designed to capture only international traffic, and would include purely domestic communications. *Id.* ¶¶ 107-11 [Vol. VI, Ex. 79, p. 2105-06]. A substantial amount of AT&T Corp.'s peered traffic in San Francisco, that is, communications between AT&T customers and non-AT&T customers, was acquired by the Surveillance Configuration, including nearly all of the peered international communications carried at the Folsom Street Facility, and a substantial amount of domestic Internet traffic. *Id.* ¶¶ 47-49; 91-111 [Vol. VI, Ex. 79, p. 2090-91, 2102-06]. According to Marcus, this web of surveillance facilities would probably capture well over half of AT&T's purely domestic traffic, representing almost all of the AT&T traffic to and from other providers. *Id.* at ¶¶ 122-127 [Vol. VI, Ex. 79, p. 2109-10].

This comprises about "*10% of all purely domestic Internet communications in the United States*," including non-AT&T customers. *Id.* at ¶¶ 125 [Vol. VI, Ex. 79, p. 2109] (emphasis in original) (evidence indicates "AT&T Corp. has given the government direct access to telecommunications facilities physically located on U.S. soil; that, by virtue of this access, the government would have the capacity to monitor both domestic and international communications of person in the United States.")

Officials briefed on the Program confirm what Klein and Marcus have said, that the surveillance starts with acquisition of all communications including content and non-content information. For example, in arguing for changes to the Foreign Intelligence Surveillance Act, Rep. Peter Hoekstra (who is read in to the Program)[11] described the technology used to conduct warrantless surveillance in the Program:

> Technology has changed dramatically from when the FISA law went into effect in 1978. The law never kept pace with technology. Right now you try to *steal light off of different cables* rather than trying to grab stuff out of the air. So that change in technology has required that for the kind of information that's most important to us, real-time collection of information, now requires a warrant.

Opsahl Decl. Ex. 14 [Vol. II, p. 714] (Interview with Rep. Peter Hoekstra by Paul Gigot, *Lack of Intelligence: Congress Dawdles on Terrorist Wiretapping,* JOURNAL EDITORIAL REPORT, FOX NEWS CHANNEL (Aug. 6, 2007) at 2) (emphasis added). The government has admitted that the Program intercepts the phone calls of Americans within the United States, though it claims to minimize after acquisition:

> Q I just have one more question. I know I'm being -- don't mean to monopolize -- but can you honestly say that no American has been wiretapped without a warrant in

---

[11] Declaration of Candace J. Morey In Support of Plaintiffs' Joint Opposition to the Motions to Dismiss by the United States and Verizon (MDL Dkt. 316) ("Morey Decl."), Ex. S [Vol. VII, Ex. 86, p. 2770-71] (Letter from John D. Negroponte, Dir. of Nat'l Intelligence, to J. Dennis Hastert, Speaker of the U.S. House of Representatives (May 17, 2006), at 2-3 (listing briefings that Rep. Hoekstra received about the Program); Opsahl Decl. Ex. 5 [Vol. I, p. 230] (*The Foreign Intelligence Surveillance Act*: Hearing before the H. Permanent Select Comm. on Intelligence, 110th Cong. 9 (Sept. 18, 2007)) (Remarks of Rep. Hoekstra: "when I became chairman of the committee [in 2004], within the first 30 days I got the call to go over to the White House because they wanted to make sure that I was fully briefed into the program and understood exactly what the programs were and the parameters.")

> this country -- has not been wiretapped -- has been wiretapped, yes, who has been wiretapped without a warrant -- warrantless wiretapping in this country.
>
> SENIOR ADMINISTRATION OFFICIAL: The reason I hesitate is because, as [my colleague] said, we will target surveillance against somebody overseas, and that person might -- 90 percent of the time that person is probably talking to people overseas, but sometimes that person is talking to somebody in the United States, and *we intercept that communication*. And as we've always done, we review that communication, and if it's irrelevant, we minimize it.

Opsahl Decl. Ex. 15 [Vol. II, p. 723] (White House Press Release, *Transcript of Background Briefing on FISA by Senior Administration Officials* (Feb. 26, 2008)) (emphasis added).

As a result of the government's data collection, "[p]articipants, according to a national security lawyer who represents one of them privately, are growing 'uncomfortable with the mountain of data they have now begun to accumulate.'" Cohn Decl. Ex. F [Vol. V, Ex. 76, p. 1747] (Barton Gellman, Dafna Linzer & Carol D. Leonnig, *Surveillance Net Yields Few Suspects: NSA's Hunt for Terrorists Scrutinizes Thousands of Americans, but Most Are Later Cleared*, WASH. POST (Feb. 5, 2006) at A01.)

2. Automated analysis, or datamining, of content and non-content information.

Once the communications are acquired, the early stages of the analysis are performed by "[c]omputer-controlled systems [that] collect and sift basic information about hundreds of thousands of faxes, e-mails and telephone calls into and out of the United States," and the last stage being actual human scrutiny. Gellman, *Surveillance Net Yields Few Suspects, supra* [Vol. V, Ex. 76, p. 1747].[12] "According to one knowledgeable source, the warrantless program . . ." uses "automated equipment to analyze the contents and guide analysts to the most important ones." *Id.* [Vol. V, Ex. 76, p. 1750]. "[T]his kind of filtering intrudes into content, and machines 'listen' to more Americans than humans do." *Id.* The Program "employ[s] extremely powerful computerized search programs—originally intended to scan foreign communications—in order to scrutinize large volumes of American communications." Cohn Decl. Ex. E [Vol. V, Ex. 76, p. 1732]; Opsahl Decl. Ex. 93 [Vol. VII] (JAMES RISEN, STATE OF WAR: THE SECRET HISTORY OF THE CIA AND THE BUSH

[12] *See also* Marcus Decl. at ¶ 39 [Vol. VI, Ex. 79, p. 2088].

ADMINISTRATION 48 (Simon & Schuster 2006) ("STATE OF WAR"); *see also* Marcus Decl. at ¶¶ 122-127 [Vol. VI, Ex. 79, p. 2109-10].

As Homeland Security Secretary Michael B. Chertoff confirmed in a January 2006 interview, the Program involves "'data-mining' – collecting vast amounts of international communications data, running it through computers to spot key words and honing in on potential terrorists." Cohn Decl. Ex. G [Vol. V, Ex. 76, p. 1753] (Morton Kondracke, *NSA Data Mining is Legal, Necessary, Chertoff Says,* ROLL CALL (Jan. 19, 2006)); *see also* Declaration of Candace J. Morey In Support of Plaintiffs' Joint Opposition to the Motions to Dismiss by the United States and Verizon (MDL Dkt. 316) ("Morey Decl."), Ex. J at 2 [Vol. VII, Ex. 86, p. 2712] (Seymour Hersh, *Listening In*, NEW YORKER (May 29, 2006) ("the N.S.A. began, in some cases, to eavesdrop on callers (often using computers to listen for key words) …")).

> One senior government official, who was granted anonymity to speak publicly about the classified program, confirmed that the N.S.A. had access to records of most telephone calls in the United States. But the official said the call records were used for the limited purpose of tracing regular contacts of "known bad guys."
>
> "To perform such traces," the official said, "you have to have all the calls or most of them. But you wouldn't be interested in the vast majority of them."

Opsahl Decl. Ex. 16 [Vol. II, p. 728] (Eric Lichtblau & Scott Shane, *Bush Is Pressed Over New Report on Surveillance*, N.Y. TIMES (May 12, 2006)); *see also* Opsahl Decl. Ex. 22 [Vol. III, p. 1043] (Letter from Kathleen Turner, Dir. of Legislative Affairs, Office of the Dir. of Nat'l Intelligence, to Rep. Silvestre Reyes, Chairman, and Rep. Peter Hoekstra, Ranking Member of the H. Intelligence Comm. ("Turner Letter"), at p. 6 of attachment) ("Intelligence analysts must comb through extremely large amounts of data to do their job.").

Even so, a recent 352-page study by the non-partisan National Research Council reports that data mining is not an effective tool in the fight against terrorism. The report's authors point to the poor quality of the data, the inevitability of false positives, the preliminary nature of the scientific evidence and individual privacy concerns in concluding that "automated identification of terrorists through data mining or any other mechanism is neither feasible as an objective nor desirable as a goal of technology development efforts." Opsahl Decl. Ex. 18 [Vol. III, p. 911-2]

(*Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention*, National Research Council, Executive Summary at 3-4 (2008)).

Regardless of the highly questionable value of datamining to our national security, prior to human review, all the acquired communications, including those to, from and/or between Americans, are stored in a vast government database. As Director of National Intelligence ("DNI") J. Michael McConnell later explained, immediately after acquisition "[t]here is no human that is aware of it. So you wouldn't know that until you went into the database." Opsahl Decl. Ex. 92 [Vol. VIII, p. 3220] (*Foreign Intelligence Surveillance Act:* Hearing before the Permanent H. Select Comm. on Intelligence, 110th Cong. 91 (Sept. 20, 2007) (statement of J. Michael McConnell, Dir. of Nat'l Intelligence (Sept. 20, 2007) ("Sept. 20, 2007, McConnell Testimony")). In testimony, DNI McConnell admitted that the communications are acquired and placed in a database *before* minimization.

> MR. MCCONNELL: … The reason is, you're collecting information. It's in a file. It will roll off in a period of time. You may not even know it's in the database. That is one of the reason we are so careful about who has access to that database. …
>
> REP. BERMAN: … How do you minimize without knowing?
>
> MR. MCCONNELL: If you look at it, then you know.
>
> REP. BERMAN: So all you do is minimize the ones you happen to look at.
>
> MR. MCCONNELL: Right. If there is something in there that -- it doesn't come up for some reason, you just wouldn't know. …

Opsahl Decl. Ex. 17 [Vol. II, p. 812] (*Warrantless Surveillance And The Foreign Intelligence Surveillance Act: The Role Of Checks And Balances In Protecting Americans' Privacy Rights (Part II)*: Hearing before the H. Comm. on the Judiciary, 110th Cong. 79 (Sept. 18, 2007)) (testimony of J. Michael McConnell, Dir. of Nat'l Intelligence) ("Sept. 18, 2007, McConnell Testimony"). Likewise, in testimony before the Senate Judiciary Committee, the following exchange took place:

> FEINSTEIN: So what is the minimization process? And how does it function? And what happens with that collection?

> MCCONNELL: The -- first of all, you may not even realize it's in the database, because you do lots of collection, you have to have a reason to look.

Opsahl Decl. Ex. 19 [Vol. III, p. 964] (Transcript of *Strengthening FISA (Foreign Intelligence Surveillance Act): Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?*: Hearing before the S. Comm. on the Judiciary, 110th Cong. 26 (Sept. 25, 2007) (testimony of J. Michael McConnell, Dir. of Nat'l Intelligence)).

The inference from DNI McConnell's statement is that U.S. person information is in the database, even if the government may initially be unaware of it. For example, while testifying before the House Intelligence Committee, DNI McConnell said "[w]e may not know that is in the database until we have some reason to go query that portion of the database for foreign intelligence purpose." Sept. 20, 2007, McConnell Testimony at 91 [Vol. VIII, Ex. 92, p. 3220]. DNI McConnell likewise explained that, initially, "you don't know what is in the database. It hasn't been examined. Remember, we are talking billions of things going on." *Id.* at 69 [Vol. VIII, Ex. 92, p. 3198]. Only "once there is some reason to look at data" can the government track the number of U.S. persons involved. *Id.* at 91 [Vol. VIII, Ex. 92, p. 3220]. McConnell also asserted that "if it were incidental, meaning they call a pizza shop, that is of no intelligence value, you take it out of the database." *Id.* at 100 [Vol. VIII, Ex. 92, p. 3229]. According to DNI McConnell, "[t]he minimization procedures that Intelligence Community agencies follow are Attorney General approved guidelines issued pursuant to Executive Order 12333. These minimization procedures apply to the acquisition, retention and dissemination of U.S. person information." Sept. 25, 2007, McConnell Testimony at 13 [Vol. III, p. 1023]; *see also* Opsahl Decl. Ex. 21 [Vol. III, p. 1030] (ODNI Minimization Attachment, at 1 ("If the collection does not contain foreign intelligence, no dissemination takes place and the data 'ages off' the system.") and 2 (whether the collection contains foreign intelligence is "not an exact science.")). *But see* March 2006 RJN, Attachment 7 [Vol. V, Ex. 77, p. 1919] (*Wartime Executive Power and the NSA's Surveillance Authority:* Hearing before the S. Comm. on the Judiciary, 109th Cong. 42 (Feb. 6, 2006) (testimony of Attorney General Alberto Gonzales, suggesting in sworn testimony before Congress that, once collected, the information is kept indefinitely, even if the subject of the surveillance is an ordinary

American: "In terms of what is actually done with that information, . . . information is collected, information is retained and information is disseminated. . . .")).

3. No minimization before acquisition, storage, data mining, or analysis by a human agent and inadequate minimization thereafter.

Domestic communications with no intelligence value are acquired and stored in the database. On the occasions where the government follows procedures established to protect Americans' privacy (obtaining a warrant or minimization by purging the record from the database), it does so not only after the communications is acquired but only after an analyst reviews the acquired communication. If a government analyst reviewed the communications and determined that "it was a U.S. person inside the United States … that would stimulate the system to get a warrant. And that is how the process would work." Sept. 20, 2007, McConnell Testimony at 70 [Vol. VIII, Ex. 92, p. 3199].[13]

In an interview with PBS's Frontline, James Baker, head of the Justice Department's Office of Intelligence Policy and Review (who is read in to the Program),[14] agreed that the following description was a "fair assessment":

> So what you're saying is that with modern communications, it's almost inevitable that you're going to collect, *in the sense of initially acquire*, communications of innocent people, of Americans who are not suspected of terrorism, but then you have to have built into the process some way of sealing them off, getting rid of them, letting them flow back into the ether.

Opsahl Decl. Ex. 23 [Vol. III, p. 2053] (Interview by PBS Frontline with James A. Baker, Counsel, U.S. Dept. of Justice (March 2, 2007)) (emphasis added).

Notably, the NSA's interpretation of what it means to "collect" communications is quite limited, such that Baker's admission that the Program collects the communications of innocent

---

[13] *See also* Opsahl Decl. Ex. 22 [Vol. II, p. 1044] (Turner Letter) at p. 7 of attachment (referencing "NSA analysts … querying Agency databases" to obtain communications to or from U.S. persons). DNI McConnell refused to provide the number of communications that get to the point of minimization in the Program, but asserted "it's a very small number considering that there are billions of transactions every day."

[14] Opsahl Decl. Ex. 5 [Vol. II, p. 307] (*The Foreign Intelligence Surveillance Act*: *Hearing before the H. Permanent Select Comm. on Intelligence*, 110th Cong. 86 (Sept. 18, 2007) (James Baker was briefed on the Program in late 2001)).

Americans is even broader than it first appears: under Department of Defense regulations, information is considered to be "collected" only after it has been "received for use by an employee of a DoD intelligence component," and "[d]ata acquired by electronic means is 'collected' only when it has been processed into intelligible form[,]" without regard to when the information was initially acquired by a surveillance device. Opsahl Decl. Ex. 24 [Vol. III, p. 1070] (Department of Defense, DOD 5240 1-R, Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons § C.2.2.1 (Dec. 1982)). In other words, the NSA actually acquires many more communications than it "collects."

Other officials defending the Program claim that:

> the NSA tries to minimize the amount of purely domestic telephone and Internet traffic among American citizens that it monitors, to avoid violating the privacy rights of U.S. citizens. But there is virtually no independent oversight of NSA's use of its new power. With its direct access to the U.S. telecommunications system, there seems to be no physical or logistical obstacle to prevent the NSA from eavesdropping on anyone in the United States that it chooses.

STATE OF WAR at 51-52 [Vol. VIII, Ex. 93]. Despite efforts at minimization, "[o]ver time, the NSA has certainly eavesdropped on millions of telephone calls and e-mail messages on American soil." *Id.* at 54.

The Wall Street Journal reported that:

> Two former officials familiar with the data-sifting efforts said they work by starting with some sort of lead, like a phone number or Internet address. In partnership with the FBI, the systems then can track all domestic and foreign transactions of people associated with that item -- and then the people who associated with them, and so on, casting a gradually wider net. An intelligence official described more of a rapid-response effect: If a person suspected of terrorist connections is believed to be in a U.S. city -- for instance, Detroit, a community with a high concentration of Muslim Americans -- the government's spy systems may be directed to collect and analyze all electronic communications into and out of the city.

Declaration of Jennifer Kelly, Ex. 19 (MDL Dkt. 441-20) [Vol VIII, Ex. 89, p. 3024] (Siobhan Gorman, *NSA's Domestic Spying Grows As Agency Sweeps Up Data*, WALL ST. J. (March 10, 2008) at A1) ("Gorman"), at 3.

In sum, the evidence shows that the NSA seeks a warrant only after the communication is (1) initially acquired; (2) placed in a government database; (3) reviewed by an analyst; and (4) the system flags it for a warrant. The telecommunications companies' assistance is complete long before any minimization.

The evidence also shows that minimization is not always used. In a January 2007 interview in the *New Yorker*, DNI McConnell noted an "[e]xception: let's suppose it was terrorism or crime. In that case, as a community, it is our obligation to report it." Opsahl Decl. Ex. 25 [Vol. III, p. 1122] (Lawrence Wright, *The Spymaster: Can Mike McConnell Fix America's Intelligence Community?*, NEW YORKER (Jan. 21, 2007)). The *New Yorker* article details a particular example in which the author's phone call to an Egyptian source was spied upon by the government. The author notes that:

> a source in the intelligence community told me that a summary of that conversation was archived in an internal database. I was surprised, because the FISA law stated that my part of the conversation should have been "minimized"—redacted or rendered anonymous—because I am an American citizen.

Id. at 1127. DNI McConnell explained to the author: "You called a bad guy, the system listened, tried to sort it out, and they did an intel report because it had foreign-intelligence value. That's our mission." *Id.*

NSA eavesdropping on conversations is not, in fact, limited to calls between Americans and non-U.S. persons. A forthcoming book by James Bamford reports, based on the eyewitness involvement of two separate NSA whistleblowers, that the agency has listened in on hundreds of US citizens overseas as they called friends and family in the United States. Opsahl Decl. Ex. 27 [Vol. III, p. 1133] (Brian Ross, et al., *Exclusive: Inside Account of U.S. Eavesdropping on Americans, U.S. Officers' "Phone Sex" Intercepted; Senate Demanding Answers*, ABC NEWS (Oct. 9, 2008)) (referencing JAMES BAMFORD, THE SHADOW FACTORY: THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA (Random House Oct. 2008) [not available to the general public in time for this summary])). One whistleblower reported that "he and others in his section of the NSA facility at Fort Gordon routinely shared salacious or tantalizing phone calls that had been intercepted, alerting office mates to certain time codes of 'cuts' that were available on each operator's computer." *Id.* The other whistleblower said that the NSA routinely listened on calls even when they knew that the participants were from international aid organizations:

> By casting the net so wide and continuing to collect on Americans and aid organizations, it's almost like they're making the haystack bigger and it's harder to find that piece of information that might actually be useful to somebody. . . ."You're actually hurting our ability to effectively protect our national security.

Id. Nor does minimization mean that private information is not available to the NSA or other government agencies: thousands of U.S. names are disclosed by the NSA to other agencies.

> [S]ince January 2004 NSA received—and fulfilled—between 3,000 and 3,500 requests from other agencies to supply the names of U.S. citizens and officials (and citizens of other countries that help NSA eavesdrop around the world, including Britain, Canada and Australia) that initially were deleted from raw intercept reports. Sources say the number of names disclosed by NSA to other agencies during this period is more than 10,000.

Opsahl Decl. Ex. 26 [Vol. III, p. 1131] (Mark Hosenball, *Spying: Giving Out U.S. Names*, NEWSWEEK (May 2, 2005)).

II. Evidence of the Telecommunications Carriers' Collaboration with the Government Program

The government could not and did not act alone. *See* Opsahl Decl. Ex. 28 [Vol. III, p. 1136] (White House Press Release, *Statement by the Press Secretary on FISA* (Feb. 25, 2008)) ("the cooperation of private entities in our intelligence operations is not ancillary - it is integral to our operations and critically essential. As Director McConnell has explained, there would be no effective surveillance without the cooperation of private partners."); *see also* September 20, 2007 McConnell Testimony at 13 [Vol. VIII, Ex. 92, p. 3142]. (The "intelligence community often needs the assistance of the private sector to protect the nation. We simply cannot go alone.")

Major U.S. telecommunications companies, including the defendants in this Multi-District Litigation, are assisting the NSA with the Program. *See* Cohn Decl. Ex. A [Vol. V, Ex. 76, p. 1707] (Leslie Cauley & John Diamond, *Telecoms Let NSA Spy On Calls*, USA TODAY (Feb. 6, 2006) ("The National Security Agency has secured the cooperation of large telecommunications companies, including AT&T, MCI and Sprint, in its efforts to eavesdrop without warrants on international calls by suspected terrorists, according to seven telecommunications executives") and Ex. B [Vol. V, Ex. 76, p. 1710] (Dionne Searcey, et al., *Wiretapping Flap Puts Phone Firms Under Fire*, WALL ST. J. (Feb. 7, 2006) at B3).

Following President Bush's Program Order, U.S. intelligence officials secretly arranged with top officials of major telecommunications companies to gain access to large telecommunications switches carrying the bulk of America's phone calls. STATE OF WAR at 48 [Vol. VII, Ex. 93]. John Yoo, the Justice Department lawyer who wrote the official legal memos purporting to legitimatize the Program, explained to Frontline:

> Q: On this issue, where do you come down -- the issue of whether or not the government needs access to the general flow of AT&T Internet and general phone calls in order to try to look for the Al Qaeda communications?
>
> Yoo: What I think the government needs [is] to have access to international communication so it can try to find communications that are coming into the country where Al Qaeda is trying to send messages to the cells members in the country. In order to do this, it does have to have access to communication networks. I think that we need to be able to move to a system where we use computers, because I think human beings can't do this one by one; you need to have computers to do it, where we have computers that are able to search through communications and are able to pluck out e-mails, phone calls that have a high likelihood of being terrorists' communications.

Opsahl Decl. Ex. 10 [Vol. I, p. 395] (Interview by PBS Frontline with John C. Yoo, Former Deputy Ass't Att'y Gen., Department of Justice (Jan. 10, 2007). According to the Senate Select Committee on Intelligence:

> [B]eginning soon after September 11, 2001, the Executive branch provided written requests or directives to U.S. electronic communication service providers to obtain their assistance with communications intelligence activities that had been authorized by the President. … The letters were provided to electronic communication service providers at regular intervals. All of the letters stated that the activities had been authorized by the President. All of the letters also stated that the activities had been determined to be lawful by the Attorney General, except for one letter that covered a period of less than sixty days. That letter, which like all the others stated that the activities had been authorized by the President, stated that the activities had been determined to be lawful by the Counsel to the President.

S.Rep. No. 110-209 at 9 (MDL Dkt. 469-2) [Vol. VIII, Ex. 90, p. 3038]. These letters were not a certification in writing under Section 2511(2)(a)(ii) of Title 18. *See* Opsahl Decl. Ex. 29 [Vol. III, p. 1144] (Transcript of *FISA Amendments: Panel I:* Hearing before the S. Comm. on the Judiciary, 110th Cong 7 (Oct. 31, 2007)) (testimony of Kenneth Wainstein)).

The evidence shows that the cooperating telecommunications companies to which these quotations refer are the defendants in this litigation. During an August 2007 interview with Chris Roberts of the *El Paso Times*, DNI McConnell admitted:

> [U]nder the president's program, the terrorist surveillance program, the *private sector had assisted us*. Because if you're going to get access you've got to have a partner and *they were being sued*. Now if you play out the suits at the value they're claimed, it would bankrupt these companies.

Verizon Plaintiffs' Second Supplemental Request for Judicial Notice (MDL Dkt. 363), Ex. E [Vol. VIII, Ex. 88, p. 3017] (Chris Roberts, *Transcript: Debate On The Foreign Intelligence Surveillance Act*, EL PASO TIMES (Aug. 22, 2007) at 2 (emphasis added)); *but see* Opsahl Decl. Ex. 30 [Vol. III, p. 1183] (Letter from J. Michael McConnell, Dir. of Nat'l Intelligence, to Rep. Peter Hoekstra, Ranking Member of the H. Permanent Select Comm. on Intelligence (Dec. 13, 2007)) (contending that "I do not believe I confirmed, nor did I intend to confirm, any specific relationship between the Government and any specific party."). Likewise, President Bush stated at a meeting with the National Governors Association on February 25, 2008, that the companies that assisted them were told that it was legal and are now being sued:

> [C]ompanies who are believed to have helped us...shouldn't be sued...Our *government told them* that their participation was necessary, and it was—and still is—and that what we had asked them to do was legal. And now *they're getting sued* for billions of dollars.

Opsahl Decl. Ex. 31 [Vol. III, p. 1187] (White House Press Release, *Transcript of President Bush Meeting with National Governors Association* (Feb. 25, 2008) (emphasis added)). Similarly, White House Press Secretary Dana Perino confirmed that the defendant telecommunications companies assisted in the Program in a press conference on February 12, 2008:

> Q: But were the telephone companies told that it was legal to wiretap six months before 9/11?
>
> MS. PERINO: The telephone companies *that were alleged to have helped* their country after 9/11 did so because they are patriotic and they *certainly helped us* and they helped us save lives.

Opsahl Decl. Ex. 32 [Vol. III, p. 1192] (White House Press Release, *Press Briefing by Dana Perino* (Feb. 12, 2008) (emphasis added)); *see also Id.* Ex. 15 [Vol. II, p. 720-27] (*Transcript of*

Background Briefing by Senior Administration Officials on FISA (Feb. 26, 2008)); *Id.* Ex. 29 [Vol. III, p. 1176] (*Transcript of FISA: Panel I*: Hearing before the S. Comm. on the Judiciary, 110th Cong 39 (Oct. 31, 2007) (Testimony of Kenneth Wainstein that "companies are rational beings, they say, okay, we cooperated before, we then got taken into court")).

The government further admitted the defendants' role in a February 2008 press statement: "Our private sector partners have serious concerns about the multibillion-dollar lawsuits some companies are currently facing … These lawsuits are abusive and, if they are allowed to proceed, would serve only to line the pockets of class-action trial lawyers." Opsahl Decl. Ex. 28 [Vol. III, p. 1136] (White House Press Release, *Statement by the Press Secretary on FISA* (Feb. 25, 2008)). The only way these lawsuits would "line the pockets" of anyone would be if the telecommunications defendants did in fact participate in the Program.

The telecommunications carrier defendants' cooperation with the Program continues. On February 27, 2008, DNI McConnell testified before the Senate Armed Services Committee. The following exchange took place:

> SEN. LEVIN: The -- Senator Inhofe raised the FISA issue. I want to just get some facts straight on this. As I understand it, last Friday night the last of the private sector partners, the telecom partners, agreed to cooperate with us. Was that true?
>
> MR. McCONNELL: We negotiated for six days and came to closure on Friday night, yes, sir.
>
> SEN. LEVIN: And so is it true then that as of last Friday night they agreed to cooperate with us?
>
> MR. McCONNELL: They did, sir.
>
> SEN. LEVIN: On a voluntary basis?
>
> MR. McCONNELL: For the subject matter as a part of the debate, the question is the uncertainty going forward. Will they do it again or --
>
> SEN. LEVIN: But as to what we were asking them to do, they agreed to do it?
>
> MR. McCONNELL: Yes, sir.

Opsahl Decl. Ex. 33 [Vol. III, p. 1207] (*Annual Threat Assessment*: Hearing before the S. Comm. on Armed Services, 110th Cong. 15 (Feb. 27, 2008) (Testimony of J. Michael McConnell)).

A. Evidence of Communications Surveillance

As early as 2001, "the NSA approached U.S. carriers and asked for their cooperation in a 'data-mining' operation, which might eventually cull 'millions' of individual calls and e-mails." Cohn Decl. Ex. D [Vol. V, Ex. 76, p. 1718] (Shane Harris and Tim Naftali, *Tinker, Tailor, Miner, Spy: Why the NSA's Snooping Is Unprecedented In Scale and Scope*, SLATE (Jan. 3, 2006)); *see also* Opsahl Decl. Ex. 34 [Vol. III, p. 1253] (Marcus Baram, *Ex-Qwest CEO: Spy Agency Retaliated Against Us, Joseph Nacchio Claims Telco Was Punished for Not Cooperating in Records Program* ABC NEWS (Oct. 12, 2007) (Nacchio "declined a NSA request to hand over Qwest customers' calling records at a Feb. 27, 2001 meeting."))

Government officials have confirmed that the NSA had obtained "backdoor access to streams of domestic and international communication" via arrangements with "some of the nation's largest telecommunications companies to gain access to [telecommunications] switches," and described the Program as a "large data-mining operation" in which NSA personnel comb "through large volumes of phone and internet traffic in search of patterns that might point to terrorism suspects." Cohn Decl. Ex. C [Vol. V, Ex. 76, p. 1714] (James Risen & Eric Lichtblau, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. TIMES (Dec. 24, 2005)). "The volume of information harvested from telecommunication data and voice networks, without court-approved warrants, is much larger than the White House has acknowledged, officials said. It was collected by tapping directly into some of the American telecommunication system's main arteries, they said." *Id.*

The NSA gained access to the vast majority of American e-mail traffic that flows through the U.S. telecommunications system. STATE OF WAR at 48 [Vol. VII, Ex. 93]. More specifically:

> NSA's technical prowess, coupled with its long-standing relationships with the nation's major telecommunications companies, has made it easy for the agency to eavesdrop on large numbers of people in the United States without their knowledge. Following President Bush's order, U.S. intelligence officials secretly arranged with top officials of major telecommunications companies to gain access to large telecommunications switches carrying the bulk of America's phone calls. The NSA also gained access to the vast majority of American e-mail traffic that flows through the U.S. telecommunications system. ...

> The new presidential order has given the NSA direct access to those U.S.-based telecommunications switches through "back doors." Under the authority of the presidential order, a small group of officials at NSA now monitors telecommunications activity through these domestic switches, searching for terrorism-related intelligence.

Id. at 48-49; *see also* Gorman at 4 [Vol VIII, Ex. 89, p. 3025] ("Current and former intelligence officials say telecom companies' concern [with this litigation] comes chiefly because they are giving the government unlimited access to a copy of the flow of communications, through a network of switches at U.S. telecommunications hubs that duplicate all the data running through it.")

Former Senator Bob Graham has said that when he was chair of the Senate Intelligence Committee in October 2002, Administration briefers told him that the President had authorized the NSA to tap into the stream of global telecommunications passing through junctions on U.S. territory, allowing the NSA to intercept "conversations that . . . went through a transit facility inside the United States." Cohn Decl. Ex. F [Vol. V, Ex. 76, p. 1748] (Barton Gellman, Dafna Linzer & Carol D. Leonnig, *Surveillance Net Yields Few Suspects: NSA's Hunt for Terrorists Scrutinizes Thousands of Americans, but Most Are Later Cleared*, WASH. POST (Feb. 5, 2006) at A01.)

B. Evidence of Call Records Surveillance

In addition, as part of the Program, the defendant telecommunications carriers have provided the call records of millions of ordinary Americans to the government. Cohn Decl. Ex. A [Vol. V, Ex. 76, p. 1706-08] (Leslie Cauley & John Diamond, *Telecoms let NSA Spy on Calls*, USA TODAY, May 11, 2006) (the "National Security Agency has been secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, Verizon and BellSouth."); Cohn Decl. Ex. C [Vol. V, Ex. 76, p. 1715] (Eric Lichtblau & James Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. TIMES, (Dec. 24, 2005), at A1 (reporting that "a former technology manager at a major telecommunications company said that since the Sept. 11 attacks, the leading companies in the industry have been storing information on calling patterns and giving it to the federal government to aid in tracking possible terrorists.")).

> One government lawyer who has participated in negotiations with telecommunications providers said the Bush administration has argued that a company can turn over its entire database of customer records — and even the stored content of calls and e-mails — because customers "have consented to that" when they establish accounts. The fine print of many telephone and Internet service contracts includes catchall provisions, the lawyer said, authorizing the company to disclose such records to protect public safety or national security, or in compliance with a lawful government request.

Opsahl Decl. Ex. 35 [Vol. III, p. 1256] (Barton Gellman & Arshad Mohammed, *Data on Phone Calls Monitored; Extent of Administration's Domestic Surveillance Decried in Both Parties*, WASH. POST (May 12, 2006) at A1); *see also* ANGLER, at 288-289 [Vol. I, Ex. 8] (discussing government attorneys' concerns about the customer consent argument).

The Program "besides actually eavesdropping on specific conversations, [has] combed through large volumes of phone and internet traffic," in a "large data-mining operation." Morey Decl. Ex. I at 1 [Vol. VII, Ex. 86, p. 2707] (Eric Lichtblau & James Risen, *Spy Agency Mined Vast Data Drove, Officials Report*, N.Y. TIMES (Dec. 24, 2005)). *See also, e.g.,* Morey Decl. Ex. J at 1 [Vol. VII, Ex. 86, p. 2711] (Seymour Hersh, *Listening In*, NEW YORKER (May 29, 2006)) (Seymour Hersh reporting that "[a] security consultant working with a major telecommunications carrier told me that his client set up a top-secret high-speed circuit between its main computer complex and . . . the site of a government-intelligence computer center," providing "total access to all the data"); Ex. K at 1 [Vol. VII, Ex. 86, p. 2715] (Lowell Bergman, Eric Lichtblau, Scott Shane, & Don Van Natta Jr., *Spy Agency Data after Sept. 11 Led F.B.I. to Dead Ends*, N.Y. TIMES (Jan. 17, 2006)); Ex. L at 1 [Vol. VII, Ex. 86, p. 2721] (Shane Harris, *NSA Spy Program Hinges on State-of-the-Art Technology*, NAT'L J. (Jan. 20, 2006)); Ex. M at 1 [Vol. VII, Ex. 86, p. 2726] (Barton Gellman, et al., *Surveillance Net Yields Few New Suspects*, WASH. POST (Feb. 5, 2006)), and Ex. N at 2 [Vol. VII, Ex. 86, p. 2734] (White House Press Release*, President Bush and Prime Minister John Howard of Australia Participate in Joint Press Availability* (May 16, 2006)). For example, AT&T was one of the telecommunications companies cooperating with the Program, and "the NSA has had a direct hookup into the database," code-named "Daytona," where AT&T "keeps track of telephone numbers on both ends of calls as well as the duration of all land-line calls." Opsahl Decl.

Ex. 36 [Vol. III, p. 1258] (Joseph Menn & Josh Meyer, *U.S. Spying is Much Wider, Some Suspect*, L.A. TIMES (Dec. 25, 2005) at A1).

When former Attorney General Gonzales defended the program in response to a question about the collection of "telephone detail records from the phone companies," he said that "what was in the *USA Today* story did relate to business records" and that "[t]here are a number of legal ways, of course, that the government can have access to business records." Morey Decl. Ex. O at 6-7 [Vol. VII, Ex. 86, p. 2745] (Dept. of Justice Press Release, *Transcript of "Operation GlobalCon" Press Conference* (May 23, 2006)). Senator Pat Roberts (who is read in to the Program)[15] characterized the collection of private customer call records as "business records" of the telecommunications companies, in an attempt to downplay the intrusion of privacy relative to the content surveillance program. His statements to Melissa Block on National Public Radio ("NPR") evidence the call records program:

> BLOCK: You're saying that you are read into it. I'm curious then if you're saying that you have had oversight directly of the program as has been reported, under which the NSA has collected millions of phone records of domestic calls.
>
> Senator ROBERTS: Well, basically, if you want to get into that, *we're talking about business records*. We're not, you know, we're not listening to anybody. This isn't a situation where if I call you, you call me, or if I call home or whatever, that that conversation is being listened to.

Id. Ex. P at 2 [Vol. VII, Ex. 86, p. 2749] (*All Things Considered: Senate Intelligence Chair Readies for Hayden Hearings* (NPR radio broadcast, May 17, 2006)) (emphasis added). Likewise, CBS News' Gloria Borger reported that Senator Roberts stated that "the NSA was looking at the phone calls collected during the surveillance, but he said not at the content, just at the pattern of phone calls." *Id.* Ex. Q at 1 [Vol. VII, Ex. 86, p. 2752] (Gloria Borger, *Congress to Be Briefed on NSA*, CBS/AP (May 16, 2006)). These statements evidence an NSA program to collect call records, in addition to the content surveillance program, under a "business records" rationale.

---

[15] *See* Morey Decl. Ex. S [Vol. VII, Ex. 86, p. 2769] (Letter from John D. Negroponte, Director of National Intelligence, to J. Dennis Hastert, Speaker of the U.S. House of Representatives (May 17, 2006), at 2-3 (listing briefings that Sen. Pat Roberts received about the Program)).

An interview with Senator Kit Bond on PBS' NewsHour also evidences the call records program:

> JIM LEHRER: … You're a member of the Senate Intelligence Committee. Did you know about this?
>
> SEN. KIT BOND, R-Mo.: Yes. I'm a member of the subcommittee of the Intelligence Committee that's been thoroughly briefed on this program and other programs….
>
> Now, to move on to the points, number one, my colleague, Senator Leahy, is a good lawyer, and I believe that he knows, as any lawyer should know, that business records are not protected by the Fourth Amendment….[16]
>
> JIM LEHRER: Excuse me, Senator Leahy, and let me just ask just one follow-up question to Senator Bond so we understand what this is about.
>
> What these are, are records. And nobody then—now, these are—but there are tens of millions of records that are in this database, right? And they say somebody, Billy Bob called Sammy Sue or whatever, and that's all it says, and then they go and try to match them with other people?
>
> SEN. KIT BOND: First, let me say that I'm not commenting on in any way any of the allegations made in the news story today. I can tell you about the president's program.
>
> The president's program uses information collected from phone companies. The phone companies keep their records. They have a record. And it shows what telephone number called what other telephone number.

Id. Ex. T at 4-5 [Vol. VII, Ex. 86, p. 2778] (*Online NewsHour Debate: NSA Wire Tapping Program Revealed,* (PBS television broadcast, May 11, 2006)). Even before the disclosures by

---

[16] Later, in August 2007, the Administration conceded that the Fourth Amendment does apply to the call records aspect of the Program:

> QUESTION: Hi. I have a couple of points that were touched on earlier, but I'm not sure really answered. On the drift net question, you talked about both the legal requirements for reasonableness under the Fourth Amendment and also just the operational logistics of using your time efficiently. Are you -- were you speaking only of surveillance where you are acquiring content, or it's your belief that those same restrictions apply to call data and tracing of call records?
> SENIOR ADMINISTRATION OFFICIAL: Well, the Fourth Amendment will apply to any of our activities. I mean, nothing is exempt from the reasonableness requirement of the Fourth Amendment.

Opsahl Decl. Ex. 37 [Vol. III, p. 1273] (Dept. of Justice Press Release, *Transcript of Conference Call with Senior Administration Officials Regarding FISA Modernization Legislation* (Aug. 7, 2007)).

Senators Roberts and Bonds, former Senate Majority Leader William Frist spoke out in defense of the call records programs to CNN's Wolf Blitzer:

> BLITZER: Let's talk about the surveillance program here in the United States since 9/11. USA Today reported a bombshell this week. Let me read to you from the article on Thursday.
>
> "The National Security Agency has been secretly collecting the phone call records of tens of millions of Americans using data provided by AT&T, Verizon and BellSouth...."
>
> Are you comfortable with this program?
>
> FRIST: Absolutely. Absolutely. I am one of the people who are briefed…[17]
>
> BLITZER: You've known about this for years.
>
> FRIST: I've known about the program. I am absolutely convinced that you, your family, our families are safer because of this particular program.

Id. Ex. U at 18 [Vol. VII, Ex. 86, p. 2800] (*Late Edition with Wolf Blitzer, Interview with Bill Frist; Interview with Stephen Hadley* (CNN television broadcast, May 14, 2006)).

In response to the uproar over the call records program reported by the *USA Today*, the White House announced that the NSA Director, Lt. General Keith Alexander, would brief the full membership of both the House and Senate Intelligence Committees on the "[f]ull terrorist surveillance program," including "the entire scope of NSA surveillance," not to be "limited to the program that the President has publicly acknowledged." Morey Decl. Ex. V at 1-2, 8 [Vol. VII, Ex. 86, p. 2817-18, 2824] (White House Press Release, *Press Briefing by Tony Snow* (May 17, 2006)). Following those briefings, *USA Today* reported that nineteen "[m]embers of the House and Senate intelligence committees confirm that the National Security Agency has compiled a massive database of domestic phone call records," and that "[t]he program collected records of the numbers dialed and the length of calls." Morey Decl. Ex. W at 1 [Vol. VII, Ex. 86, p. 2831] (Susan Page, *Lawmakers: NSA Database Incomplete*, USA TODAY (June 30, 2006)). Further, several members of Congress spoke on the record. Senator Saxby Chambliss, bemoaning BellSouth's alleged refusal to participate, opined that "[i]t probably would be better to have records of every telephone company." *Id*. at 2 [Vol. VII, Ex. 86, p. 2832]. According to Senator Ted Stevens, the records program targeted long-distance, not "cross-city" or "mom-and-pop calls." *Id.* Senator Orrin Hatch, Rep. Anna Eshoo, and Rep. Rush Holt also made statements on the record acknowledging the program. *Id*. at 3 [Vol. VII, Ex. 86, p. 2833].

---

[17] Morey Decl. Ex. S [Vol. VII, Ex. 86, p. 2770-71] (Letter from John D. Negroponte, Dir. of Nat'l Intelligence, to J. Dennis Hastert, Speaker of the U.S. House of Representatives (May 17, 2006), at 2-3 (listing briefings that Sen. Frist received about the Program)).

Separately, Representative Jane Harman has noted that "there is a program that involves the collection of some phone records." Morey Decl. Ex. X at 8 [Vol. VII, Ex. 86, p. 2843] (*The Department of Homeland Security State and Local Fusion Center Program: Advancing Information Sharing while Safeguarding Civil Liberties:* Hearing of the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment of the H. Homeland Security Comm., 110th Cong. (2007) (statement of Rep. Jane Harman)). This makes nine members of Congress, each fully briefed on "the entire scope of NSA surveillance,"[18] who have acknowledged the call records program publicly and on-the-record.

As noted in this Court's *Hepting* decision, Qwest has unequivocally confirmed requests by the government for "private telephone records of Qwest customers," which Qwest refused after learning that it would not be provided with any lawful authority permitting such access. *Hepting v. AT&T,* 439 F. Supp. 2d at 988; *see also* Morey Decl. Ex. Y at 1 [Vol. VII, Ex. 86, p. 2854] (*Full Statement From Attorney Of Former Qwest CEO Nacchio,* WALL ST. J. ONLINE (May 12, 2006)). According to Joseph Nacchio, "Chairman and CEO of Qwest [who] was serving pursuant to the President's appointment as the Chairman of the National Security Telecommunications Advisory Committee," the refusal to comply was based on a "disinclination on the part of the authorities to use any legal process" in support of the request. *Id.*; *see also* Opsahl Decl. Ex. 94 [Vol. VIII, p. 3240] (Scott Shane, *Former Phone Chief Says Spy Agency Sought Surveillance Help Before 9/11*, N.Y. TIMES (Oct. 14, 2007) (Former Qwest CEO asserts that Qwest refused a government request for surveillance assistance in February 2001)).

---

[18] Rep. Harman is a member of the subcommittee that received numerous briefings on the NSA programs on at least eight occasions. Morey Decl. Ex. S [Vol. VII, Ex. 86, p. 2770-71] (Letter from John D. Negroponte, Director of National Intelligence, to J. Dennis Hastert, Speaker of the U.S. House of Representatives (May 17, 2006), at 2-3).

In April 2007, Verizon Wireless admitted it was asked by the government to hand over private phone records, through a pre-recorded statement by a Regional President, Kelly Kurtzman, reported by Lee Hochberg on PBS's NewsHour:

> LEE HOCHBERG: Privacy advocate Hendricks . . . notes, after 9/11, the Bush administration asked phone companies for billions of private phone records.
>
> Federal law forbids turning them over without a court order, but most phone companies did so anyway. Verizon's landline division was hit with a $50 billion consumer lawsuit for doing so. Verizon Wireless emphasizes it withheld its phone records.
>
> KELLY KURTZMAN: Absolutely, absolutely. We were asked, but we said, no, we would not give that information, again, you know, trying to protect the privacy of our customers. We take that very seriously.

Morey Decl. Ex. Z at 3 [Vol. VII, Ex. 86, p. 2858] (*Online NewsHour: New Cell Phone Technology Can Track Users,* (PBS television broadcast, April 11, 2007)). This shows that the government had asked wireless telephone providers, like defendant Cingular, to participate in the Program.

The government's 2007 reports on the FBI's call record collections further confirm the defendant telecommunications companies' disclosure of call detail information to the government. The FBI's general counsel, Valerie Caproni, testified before Congress that AT&T, Verizon and MCI have current contracts with the FBI to provide telephone toll records. Morey Decl. Ex. HH at 45 [Vol. VII, Ex. 86, p. 2945] (*The Inspector General's Independent Report on the F.B.I.'s Use of National Security Letters*: Hearing Before the H. Judiciary Comm., 110th Cong. (2007) ("IG's Report Hearing") (testimony of Valerie Caproni, FBI General Counsel and Glenn A. Fine, DOJ Inspector General)). She confirmed details revealed by a March 2007 report by the DOJ's Office of Inspector General (Morey Decl. Ex. II [Vol. VII, Ex. 86, p. 2987] ("IG's Report")) about numerous abuses by Verizon, MCI and AT&T in turning over reams of telephone toll records. These contracts enabled Verizon and MCI to "provide 'near real-time servicing'" of records requests and meet the FBI's need to quickly obtain billing data. *Id*. at 88; *see also* Opsahl Decl. Ex. 38 [Vol. III, p. 1277] (Ryan Singel, *FBI Seeking to Pay Telecoms to Store Records for Years and Provide Instant Access*, WIRED NEWS (July 18, 2007)).

Furthermore, "one of the [IG's] most troubling findings" was that the "FBI improperly obtained telephone toll billing records and subscriber information from three telephone companies [Verizon, MCI and AT&T] pursuant to over 700 so-called exigent letters." IG Report Hearing at 10 [Vol. VII, Ex. 86, p. 2910] (Testimony of Glenn A. Fine, Inspector General, Dept. of Justice). In response to these exigent letters, the carriers provided call records to the FBI prior to receiving either a National Security Letter ("NSL") or a grand jury subpoena. *See* IG's Report at 89-90 [Vol. VII, Ex. 86, p. 2988-89].

Indeed, the Inspector General noted use of NSLs to access information about individuals who are "two or three steps removed from their subjects without determining if these contacts reveal suspicious connections." *Id.* at 109 (emphasis added) [Vol. VII, Ex. 86, p. 2993]; *see also* Opsahl Decl. Ex. 39 [Vol. III, p. 1280] (Eric Lichtblau, *F.B.I. Data Mining Reached Beyond Initial Targets*, N.Y. TIMES (Sept. 9, 2007) ("The F.B.I. cast a much wider net in its terrorism investigations than it has previously acknowledged by relying on telecommunications companies to analyze phone-call patterns of the associates of Americans who had come under suspicion, according to newly obtained bureau records.")). Accordingly, the evidence shows that while the telecommunications companies provided call-detail records to the government, it was not pursuant to the NSL statute, 18 U.S.C. § 2709.

C. Evidence that AT&T Participated in the Program

1. Evidence of AT&T's collaboration with the communications acquisition aspect of the Program

AT&T Corp. (now a subsidiary of AT&T Inc.) maintains domestic telecommunications facilities over which millions of Americans' telephone and Internet communications pass every day. Klein Decl. ¶ 7 [Vol. V, Ex. 78, p. 2041]; *see generally* Cohn Decl. Exs. H and I [Vol. V, Ex. 76, p. 1755-62] (*The AT&T Advantage, First Quarter 2004* and *SBC Investor Briefing*, January 31, 2005, No. 246). These facilities allow for the transmission of interstate or foreign electronic voice and data communications by the aid of wire, fiber optic cable, or other like connection between the point of origin and the point of reception. Klein Decl. ¶ 7 [Vol. V, Ex. 78, p. 2041].

Former AT&T technician Mark Klein has provided this Court with detailed evidence proving that AT&T has been collaborating with the NSA in the surveillance of the domestic communications of millions of Americans. Klein's account begins around January 2003, when the manager of his facility advised him that the NSA was coming to interview another colleague for a "special job." Klein Decl. ¶ 10 [Vol. V, Ex. 78, p. 2042]. The "special job" was to install equipment in a high-security room AT&T was building at its Folsom Street Facility in San Francisco. *Id.* ¶ 10-14 [Vol. V, Ex. 78, p. 2042]. The NSA supervised the construction and outfitting of the room, which came to be known as the "SG3 Secure Room." *Id.* ¶ 12 [Vol. V, Ex. 78, p. 2042]. Klein personally saw the room when it was under construction, and, at one point, entered the room briefly after it was fully operational. *Id.* ¶ 12, 17 [Vol. V, Ex. 78, p. 2042, 2043].

In October 2003, AT&T transferred Klein to the Folsom Street Facility. *Id.* ¶ 15 [Vol. V, Ex. 78, p. 2042]. Although AT&T entrusted Klein with keys to every other door at the Folsom Street Facility, he did not have access to the SG3 Secure Room. *Id.* ¶ 17 [Vol. V, Ex. 78, p. 2043]. No AT&T employee was allowed in the secret room without NSA security clearance. *Id.* Klein recounts one event that underscores the "extremely limited access to the SG3 Secure Room": A large industrial air conditioner in the room began "leaking water through the floor and onto . . . equipment downstairs." *Id.* ¶ 18 [Vol. V, Ex. 78, p. 2043]. AT&T maintenance personnel were not allowed to enter to fix the leak—or even to triage and prevent water damage to other portions of the facility. *Id.* Despite the "semi-emergency," AT&T waited days for a repairman with NSA clearance to provide service. *Id.*

At the Folsom Street Facility, Klein's job was to oversee AT&T's "WorldNet Internet room." *Id.* ¶ 15 [Vol. V, Ex. 78, p. 2042]. Communications carried by AT&T's WorldNet Internet service pass through that room to be directed to or from customers. *Id.* ¶ 19 [Vol. V, Ex. 78, p. 2043]. The WorldNet Internet Room is designed to process vast amounts of electronic communications traffic "peered"[19] by AT&T Corp. between its Common Backbone ("CBB")[20]

[19] "Peering" is the process whereby Internet providers interchange traffic destined for their respective customers, and for customers of their customers. *See* Marcus Decl. ¶¶ 96-98 [Vol. VI, Ex. 79, p. 2102-2103].

Internet network and other carriers' networks. Klein Decl. ¶ 22 [Vol. V, Ex. 78, p. 2044]. The Folsom Street Facility also handles millions of telephone communications. *Id.* ¶ 13 [Vol. V, Ex. 78, p. 2042].

Klein revealed that AT&T intercepts every single one of the communications passing through the WorldNet Internet room and directs them all to the NSA. Klein Decl. ¶¶ 22-36 [Vol. V, Ex. 78, p. 2044-46]. As Klein explained, the communications are carried as light signals on fiber-optic cables. *Id.* ¶¶ 21-24 [Vol. V, Ex. 78, p. 2044]. To divert the communications, AT&T connected the fiber-optic cables entering the WorldNet Internet room to a "splitter cabinet." *Id.* ¶¶ 25-34 [Vol. V, Ex. 78, p. 2044-2045]. The splitter cabinet splits the light signals from the WorldNet Internet service in two, making two identical copies of the material carried on the light signal. *Id.* The splitter cabinet directed one portion of the light signal through fiber optic cables into the NSA's secret room while allowing the other portion to travel its normal course to its intended destination. *Id.* ¶¶ 27-34 [Vol. V, Ex. 78, p. 2044-2045]. The split cables carried domestic and international communications of AT&T customers, as well as communications from users of other non-AT&T networks that pass through the Folsom Street Facility. *Id.* ¶¶ 31-34 [Vol. V, Ex. 78, p. 2045].

Klein attached to his declaration two AT&T documents called "SIMS Splitter Cut-In and Test Procedure," which describe "how to connect the already in-service circuits to a 'splitter cabinet,' which diverted light signals from the WorldNet Internet service's fiber optical circuits to the SG3 Secure Room." Klein Decl. ¶ 26 and Exs. A & B [Vol. V, Ex. 78, p. 2044, 2047-2052, 2053-2058]. He also attached a third AT&T document "describ[ing] the connections from the SG3 Secure Room on the 6th floor to the WorldNet Internet room on the 7th floor, and provid[ing] diagrams on how the light signal was being split." Klein Decl. ¶ 28 and Ex. C [Vol. V, Ex. 78, p. 2045, 2059-2069]. This document also "listed the equipment installed in the SG3 Secure Room."

---

[20] AT&T's Common Backbone network, like backbone networks generally, is used for the transmission of interstate or foreign communications. An Internet backbone can be thought of as a large ISP, many of whose customers may themselves be smaller ISPs. There is no single network that is ***the Internet***; rather, the Internet backbones collectively form the core of the global Internet. *See* Marcus Decl. nn. 5-6, at 3 [Vol. V, Ex. 78].

Klein Decl. ¶ 35 [Vol. V, Ex. 78, p. 2045]. These three documents comprise over 100 pages of highly technical details on the interceptions, including 57 detailed schematics and 24 tables of data.

James Russell, AT&T's Managing Director-Asset Protection, has confirmed that Klein's declaration and the AT&T documents Klein attached accurately describe AT&T's Internet network, AT&T's San Francisco communications facility and the location of specific equipment within the San Francisco facility, and the interconnection points of AT&T's Internet network with the networks of other communications carriers. Declaration of James W. Russell (Hepting Dkt. 41), at 1-2, 4-7. Russell confirmed the conclusion that the exhibits to the Klein Declaration are authentic AT&T documents that provide "detailed schematics of network wiring configurations that are uniform across AT&T locations and that are used by AT&T to cross-connect and split fiber cables" and "identif[y] the manufacturer and name of many pieces of equipment used by AT&T." Russell Decl. at 7.

Plaintiffs' expert J. Scott Marcus confirmed "Mr. Klein's allegation that the room described was a secure facility, intended to be used for purposes of surveillance on a very substantial scale." Marcus Decl. ¶ 6 [Vol. VI, Ex. 79, p. 2082]. He "conclude[d] that AT&T has constructed an extensive—and expensive—collection of infrastructure that collectively has all the capability necessary to conduct large scale covert gathering of IP-based communications information, *not only for communications to overseas locations, but for purely domestic communications as well.*" Marcus Decl. ¶ 38 [Vol. VI, Ex. 79, p. 2088] (emphasis in original). "This deployment," he opines, "*is neither modest nor limited.*" Marcus Decl. ¶ 43 [Vol. VI, Ex. 79, p. 2090] (emphasis in original).

The expert further concluded that "all or substantially all" of AT&T's "peered traffic" in San Francisco was sent into the SG3 Secure Room, *Id.* ¶ 108 [Vol. VI, Ex. 79, p. 2105], meaning any communication between AT&T customers and non-AT&T customers. *Id.* ¶¶ 91-108 [Vol. VI, Ex. 79, p. 2102-05]. AT&T made no effort to filter out purely domestic-to-domestic electronic communications, as a fiber splitter is not a selective device; all traffic on the split circuit was diverted or copied. *Id.* ¶¶ 109-112 [Vol. VI, Ex. 79, p. 2105-07].

Klein's evidence establishes AT&T's participation in the Program at its San Francisco location, but there is more. From the arrangement of the hardware, plaintiffs' expert Marcus concluded that AT&T's surveillance "apparently involves considerably more locations than would be required to catch the majority of international traffic." Marcus Decl. ¶ 43 [Vol. VI, Ex. 79, p. 2090]. Further evidence confirms the expert's view. Klein reports "that other such 'splitter cabinets' were being installed in other cities, including Seattle, San Jose, Los Angeles and San Diego." Klein Decl. ¶ 36 [Vol. V, Ex. 78, p. 2046]; *see also* Gorman at 7 [Vol. VIII, Ex. 89, p. 3028] ("Current and former intelligence officials confirmed a domestic network of hubs, but didn't know the number.") At AT&T's Bridgton technical command center in St. Louis, "AT&T has maintained a secret, highly secured room since 2002 where government work is being conducted" and that "only government officials or AT&T employees with top-secret security clearance are admitted to the room." Decl. of Cindy Cohn in Support of Opp. to Motion to Stay (MDL Dkt. 129) ("Second Cohn Decl."), Ex. 1 [Vol. VI, Ex. 82, p. 2453] (Kim Zetter, *Is the NSA spying on U.S. Internet traffic?*, SALON MAGAZINE (June 21, 2006)).

James Cicconi, AT&T's senior executive vice president for external and legislative affairs, said, on August 22, that there are "very specific federal statutes that prescribe means, in black and white law, for provision of information to the government under certain circumstances. ... We have stringently complied with those laws." As Cicconi said, "[i]t's pretty obvious, you know, as far as the court case is going, that they've not reached a different conclusion." Second Cohn Decl. Ex. 2 [Vol. VI, Ex. 83, p. 2458] (Declan McCullagh, *AT&T Says Cooperation with NSA Could Be Legal*, CNET NEWS (Aug. 22, 2006)). This statement is nonsensical unless AT&T is participating in the program.

According to the plaintiffs' expert Marcus, the Surveillance Configuration is consistent with the media reports describing telecommunications companies' assistance with the Program, and illustrates an infrastructure built and designed by AT&T Corp. to conduct covert collection and intensive analysis of substantial amounts of both international and domestic Internet communications carried by AT&T Corp.'s network, including domestic communications of AT&T

WorldNet Internet service customers such as the plaintiffs. *See* Marcus Decl. ¶¶ 37-49 [Vol. VI, Ex. 79, p. 2088-91].

Accordingly, the Klein Declaration and exhibits attached thereto, the Marcus Declaration, and the numerous news media accounts show that AT&T has built the capability necessary to conduct large-scale covert surveillance of electronic communications, and is providing the NSA with direct access to this capability as part of its ongoing and illegal collaboration with the government's warrantless surveillance Program.

2. Evidence of AT&T's collaboration with the call detail records aspect of the Program

AT&T also gave the government call-detail records without proper legal authorization. At a 2006 hearing before the Senate Judiciary Committee, Edward Whitacre, CEO of AT&T, responded to a question on the call-detail records aspects of the Program by saying "if it's legal, we do it." *The AT&T And Bellsouth Merger: What Does It Mean For Consumers?:* Hearing before the Subcomm. on Antitrust, Competition Policy and Consumer Rights of the S. Comm. on the Judiciary, 109th Cong. (2d Sess.) 13 (June 22, 2006); *see also Hepting v. AT&T,* 974 F.Supp.2d at 993 ("Hence, it appears AT&T helps the government in classified matters when asked and AT&T at least currently believes, on the facts as alleged in plaintiffs' complaint, its assistance is legal.") In 2007, when responding to the House Energy & Commerce Committee, AT&T wrote that "the President possesses independent authority to request intelligence assistance pursuant to his" Article II powers. Opsahl Decl. Ex. 98 [Vol. VIII, p. 3476] (Letter from Wayne Watts, Senior Executive Vice President and General Counsel, AT&T, to Reps. John Dingell, Edward Markey and Bart Stupak (Oct. 12, 2007), at 5). Thus, AT&T opined, it would be legal for the government to "request various forms of intelligence assistance from the private sector pursuant to Executive Order 12333 and/or the President's Article II powers upon which that Order rests." *Id.*

D. Evidence that Verizon Participated in the Program

Verizon issued a press release on May 12, 2006 stating that, because the call records program was highly classified, Verizon could not "confirm or deny whether we have had any relationship to it." Morey Decl. Ex. AA at 1 [Vol. VII, Ex. 86, p. 2861] (News Release, *Verizon*

Issues Statement on NSA and Privacy Protection (May 12, 2006)). As to MCI, it stated: "In January 2006, Verizon acquired MCI, and we are ensuring that Verizon's policies are implemented at that entity and that all its activities fully comply with law." *Id*. (emphasis added).

As popular uproar over the call records program grew, Verizon issued a second statement four days later in a very different tone. That May 16 statement expressly denied that "Verizon" brand businesses had turned over call records, but tacitly admitted MCI's participation. Morey Decl. Ex. BB at 1 [Vol. VII, Ex. 86, p. 2863] (News Release, *Verizon Issues Statement on NSA Media Coverage*, (May 16, 2006)). Describing the actions of the company prior to Verizon's January 2006 acquisition of MCI, it explained:

> From the time of the 9/11 attacks until just four months ago, Verizon had three major businesses-its wireline phone business, its wireless company and its directory publishing business. It also had its own Internet Service Provider and long-distance businesses. Contrary to the media reports, Verizon was not asked by NSA to provide, nor did Verizon provide, customer phone records from any of *these businesses*, or any call data from *those records*. None of *these companies* -wireless or wireline - provided customer records or call data.

Id. (emphasis added). Pressed on the point, Peter Thonis, Verizon's chief communications officer, said the May 12, 2006 denial of participation in the call records program was about Verizon, not MCI. *See* Morey Decl. Ex. CC at 1-2 [Vol. VII, Ex. 86, p. 2866-67] (Jim Drinkard, *Verizon Says It Isn't Giving Call Records to NSA*, USA TODAY (May 16, 2006)). Verizon's earlier promise to ensure that its policies "are implemented" at MCI, with Verizon's calculated exclusion of MCI from its public denial of involvement must fairly be read as an admission of MCI's participation in the call records program.[21]

---

[21] Further, Verizon customer service representatives have told customers that Verizon turned over call records of Verizon wireline customers to the NSA. *See, e.g.,* Verizon Plaintiffs Master Consolidated Complaint (MDL Dkt. 125) ("MCC") ¶ 184(3) (on May 11, 2006, a "customer service representative told [Michael Colonna of New Jersey] that although the records of other Verizon customers were disclosed, the records of Verizon wireless customers were not disclosed;" MCC ¶ 184(1) (on May 12, 2006, Verizon customer service representative Ellen "expressly confirmed to [landline customer Norman LeBoon of Pennsylvania:] . . . 'I can tell you Mr. LeBoon that your records have been shared with the government, but that's between you and me'"); MCC ¶ 184(2) (Verizon customer service representative on May 16, 2006 told Verizon subscriber Mark Baker that "Verizon has turned its subscriber records over to the NSA").

MCI's participation was also confirmed in the June 30, 2006, *USA Today* story that followed the full briefing of all members of the Intelligence Committees on all aspects of the NSA's surveillance activities. Morey Decl. Ex. W at 1-2 [Vol. VII, Ex. 86, p. 2831-32]. Four intelligence committee members verified that "MCI, the long-distance carrier that Verizon acquired in January, did provide call records to the government," while "[f]ive members of the intelligence committees said they were told by senior intelligence officials that AT&T participated in the NSA domestic calls program." *Id.*. And, like AT&T, MCI plays a critical role in the long distance and international calling infrastructure targeted under the NSA programs. Before the merger, MCI was the second largest long distance carrier with "14 million residential customers and about a million corporate customers." Morey Decl. Ex. DD at 1 [Vol. VII, Ex. 86, p. 2870] (Matt Richtel & Andrew R. Sorkin, *Verizon Agrees to Acquire MCI For $6.6 Billion, Beating Qwest*, N.Y. TIMES (Feb. 14, 2005)). In 2003, MCI received 20.8 percent of all long distance toll service revenues, trailing only AT&T. Morey Decl. Ex. EE at 9-11, 9-12 [Vol. VII, Ex. 86, p. 2880-81] (Excerpts of *FCC Industry Analysis and Technology Division Wireline Competition Bureau, Trends in Telephone Service* (June 21, 2005)). Indeed, a majority of international calls are handled by long-distance carriers AT&T, MCI, and Sprint. Cohn Decl. Ex. A [Vol. V, Ex. 76, p. 1707] (Leslie Cauley and John Diamond, *Telecoms Let NSA Spy on Calls*, USA TODAY (Feb. 6, 2006)).

Verizon's ubiquity in providing telecommunications services is also beyond dispute. As of year-end 2006, Verizon's wireline network included more than 45 million access lines nationwide, with approximately 13 million miles of local, inter-city and long-distance fiber-optic systems. Morey Decl. Ex. GG at 4 [Vol. VII, Ex. 86, p. 2891] (Recent Verizon History, printed on June 21, 2007).

While Verizon doubtless received substantial numbers of NSLs, the evidence shows that this is insufficient for a certification pursuant to Section 802(a)(3). Verizon has said that "Verizon has not provided assistance to the government to conduct a wiretap *based on an NSL*." Opsahl Decl. Ex. 40 [Vol. III, p. 1284] (Letter from Randal S. Milch, Senior Vice President, Legal & External Affairs & General Counsel, Verizon to Reps. John Dingell, Edward Markey and Bart

Stupak (Oct. 12, 2007) at 3 (emphasis added)); *see also id.* at 13 (denying providing calling circle information to the government in response to NSLs).

III. The Evolution of the Program Over Time

This section summarizes several significant events in the history of the Program. In March 2004, the legal theories that purported to support the Program became more widely known within the Administration, leading to very serious disagreements, and nearly causing the resignation of several senior officials. In January 2007, the Program was purportedly authorized by the Foreign Intelligence Surveillance Court ("FISC") (though the operations remained unchanged), until the FISC reconsidered and found the Program illegal a few months later. In August 2007, Congress passed new legislation relating to electronic surveillance.

A. March 2004 Administration Revolt Over Illegal Surveillance

According to then-Attorney General Gonzales, the legality of the intelligence activities authorized by the President in the Program Order, beyond those aspects later marketed as the Terrorist Surveillance Program ("TSP"), was a matter of "very serious disagreement." Verizon Plaintiffs Request for Judicial Notice (MDL Dkt. 356) ("Verizon RJN"), Ex. D (Letter from Alberto R. Gonzales, Att'y Gen. of U.S., to Sen. Patrick Leahy, Chairman, S. Comm. on the Judiciary (Aug. 1, 2007), at 2). In March 2004, "when the presidential order was set to expire, the Department of Justice, under Acting Attorney General James Comey, refused to give its approval to the reauthorization of the order because of concerns about the legal basis of certain of these NSA activities," but that DOJ approval was granted again later in the spring of 2004 after a "thorough reexamination" by the DOJ of the NSA's activities. *Id.; see generally* Opsahl Decl. Ex. 57 [Vol. IV] (*Preserving Prosecutorial Independence: Is the Department of Justice Politicizing the Hiring and Firing of U.S. Attorneys?* Hearing before the S. Comm. on the Judiciary, Part IV, 110th Cong. (May 15, 2007) ("Comey Testimony")).

The legal justifications for the NSA warrantless surveillance program caused considerable internal disagreement. "One source familiar with the NSA program said yesterday that there were widespread concerns inside the intelligence community in 2003 and 2004 over how much Internet and telephone data mining could occur, as well as about the NSA's direct intercepts of communications without court approval." Opsahl Decl. Ex. 41 [Vol. III, p. 1296] (Dan Eggen & Joby Warrick, *Data Mining Figured In Dispute Over NSA, Report Links Program to Gonzales Uproar*, WASH. POST (July 29, 2007) at A04.) "What the NSA was casting as a carefully targeted surveillance operation struck some officials as a vast data mining operation run amok, with the NSA combing through vast volumes of 'meta-data' to trace and analyze phone and e-mail traffic across the United States." BUSH'S LAW AT 178 [Vol. I, Ex. 1]. It started with Deputy Assistant Attorney General Patrick Philbin. Philbin, who was read into the Program in mid-2003, was concerned because "[o]n its face, the program violated two felony statutes forbidding electronic surveillance without a warrant [and the] specified exceptions in those statutes did not apply." ANGLER at 288 [Vol. I, Ex. 8]. By the fall of 2003, Jack Goldsmith, then head of the Justice Department's Office of Legal Counsel, and Philbin began a factual and legal review of the Program. Comey Testimony at 245 [Vol. IV, Ex. 57, p. 1542]. Goldsmith later testified that there were certain "aspects of programs related to the TSP that I could not find legal support for," describing the basis as "a legal mess. It was the biggest legal mess I've ever encountered." Opsahl Decl. Ex. 42 [Vol. IV, p. 1307] (*Preserving the Rule of Law in the Fight Against Terror:* Hearing before the S. Comm. on the Judiciary, 110th Cong. 7 (Oct. 2, 2007) (testimony of Jack Goldsmith)); *see also* THE TERROR PRESIDENCY AT 180-82 [Vol. I, Ex. 9].

On Tuesday, March 9, 2004, Comey orally advised Administration officials that he saw no legal basis for certain aspects of the activities subject to reauthorization. Opsahl Decl. Ex. 55 [Vol. IV, p. 1494] (Memorandum from Alberto Gonzales, Fmr. Att'y Gen. of the U.S., *Concerning the Report of Investigation Regarding Allegations of Mishandling of Classified Documents by Fmr. Att'y Gen. Alberto Gonzales* (Aug. 28, 2008) at 7 ("OIG Gonzales Report"); *see also* Comey Testimony at 246, 248 [Vol. IV, Ex. 57, p. 1543, 1545]. This conversation led to a heated dispute between Comey and Addington:

> An imposing former prosecutor and self-described conservative who stands 6-foot-8, [Comey] was the rare administration official who was willing to confront [Cheney's Chief of Staff and Legal Counsel David] Addington. At one testy 2004 White House meeting, when Mr. Comey stated that "no lawyer" would endorse

> [John] Yoo's justification for the N.S.A. program, Mr. Addington demurred, saying he was a lawyer and found it convincing. Mr. Comey shot back: "No good lawyer," according to someone present.

Opsahl Decl. Ex. 43, [Vol. IV, p. 1357] (Scott Shane, et al., *Secret U.S. Endorsement of Severe Interrogations*, N.Y. TIMES (Oct. 4, 2007)); *see also* ANGLER at 296 [Vol. I, Ex. 8] ("'The analysis is flawed, in fact facially flawed,' Comey said. 'No lawyer reading that could reasonably rely on it.'").

At the time, Comey was the Acting Attorney General, because Attorney General John D. Ashcroft was hospitalized at George Washington University Hospital. *See* ANGLER at 302-307 [Vol. I, Ex. 8]; *see also* Comey Testimony at 250 [Vol. IV, Ex. 57, p. 1547]. Comey would not sign off on the legality of the Program. Comey Testimony at 224 [Vol. IV, Ex. 57, p. 1521]; *see also* OIG Gonzales Report at 9 [Vol. I, Ex. 7, p. 355]; and BUSH'S LAW at 180 [Vol. I, Ex. 1].

On March 10, 2004, "Gonzales and other White House and intelligence agency officials, including the Vice President and NSA Director Michael Hayden, convened an 'emergency meeting' in the White House Situation Room with" Congresses' Gang of Eight.[22] OIG Gonzales Report at 9 [Vol. I, Ex. 7, p. 355]; *see also* Morey Decl. Ex. S [Vol. VII, Ex. 86, p. 2770-71] (Letter from John D. Negroponte, Dir. of Nat'l Intelligence, to J. Dennis Hastert, Speaker of the U.S. House of Representatives (May 17, 2006) at 2-3 (listing congressional participants). Accounts of this meeting differ significantly. *See* Opsahl Decl. Ex. 44, [Vol. IV, p. 1378] (Dan Eggen & Paul Kane, *Gonzales, Senators Spar on Credibility, Account of Meeting In '04 Is Challenged*, WASH. POST (July 25, 2007) at A01); ANGLER AT 300-301 [Vol. I, Ex. 8]. Gonzales wrote notes concerning this meeting, which "were reviewed by two NSA officials" in conjunction with a 2008 investigation into Gonzales' mishandling of classified material. OIG Gonzales Report at 10 n.14 [Vol. I, Ex. 7, p. 365]. "The NSA officials determined that 3 of 21 paragraphs in the notes contain SCI information about the NSA surveillance program, 1 paragraph contains SCI information about signals intelligence, and the remaining paragraphs are unclassified." *Id.*

---

[22] The Gang of Eight refers to congressional leadership, including the leaders of each of the two parties from each of the two houses of Congress and the chairs and ranking members of the intelligence committees of each of the two houses of Congress. *See* http://en.wikipedia.org/wiki/Gang_of_eight.

On the night of March 10, 2004, Gonzales and White House Chief of Staff Andrew Card attempted to go around Comey, and sought Ashcroft's certification on his hospital bed. ANGLER at 302-303 [Vol. I, Ex. 8]; BUSH'S LAW at 180-181 [Vol. I, Ex. 1]; Comey Testimony at 215-17 [Vol. IV, Ex. 57, pp. 1512-1514]. Comey got word of the impending hospital visit while driving home, made a U-turn on Constitution Avenue, and rushed to Ashcroft's side with the emergency lights flashing. *Id.* However, instead of signing the Program Order, "Ashcroft gave a lucid account of the reasons that Justice had decided to withhold support. And then he went beyond that. Ashcroft said he never should have certified the program." ANGLER at 304 [Vol. I, Ex. 8]; BUSH'S LAW at 182 [Vol. I, Ex. 1]. "Ashcroft specified a list of facts, and a list of legal concerns, that the secrecy rules had prevented him from discovering. Had he known them, he said, he would have withheld his signature before." ANGLER at 459 [Vol. I, Ex. 8, p. 385].

When Gonzales testified about the hospital incident in July 2007, he refused to directly say that the former Attorney General approved the Program for the first two years, despite heavy questioning. Instead, Gonzales testified that "from the inception, we *believed* that we had the approval of the attorney general of the United States for these activities, these particular activities." Opsahl Decl. Ex. 45, [Vol. IV, p. 1417] (*Oversight of the Department of Justice*: Hearing before the S. Comm. on the Judiciary, 110th Cong. 33-35 (July 24, 2007)) (emphasis added). Gonzales' parsing of words is further evidence that Ashcroft was highly concerned about the program. Gonzales also noted that Aschroft's explanation of his concerns did not require classified information. *Id.* at 1415; *see also* Comey Testimony at 247 [Vol. V, Ex. 57, p. 1544] ("I don't believe that [Ashcroft] disclosed classified information in the hospital room.")

Despite the conclusion by the Department of Justice that the Program violated criminal laws, Bush nevertheless reissued the Program Order on or around March 11, 2004. ANGLER at 312-13 [Vol. I, Ex. 8]; Comey Testimony at 218-19 [Vol. V, Ex. 57, pp. 1515-1516]. "Addington deleted the Justice Department from the document [and] typed in 'Alberto R. Gonzales,' the White House Counsel, on a substitute signature line." ANGLER at 311 [Vol. I, Ex. 8]. "He did not stop at adding a legally meaningless signature line for Gonzales. Addington drew up new language in which Bush relied upon his own authority to certify the program as lawful. … The rewritten directive declared in sweeping terms that Bush had the final word. Addington's formula may have been the nearest thing to a claim of unlimited power ever made by an American president." *Id.* at 312-313.

As a result of this incident, about "two dozen Bush appointees," including Acting Attorney General Comey and FBI Director Mueller, were prepared to resign. *See* Comey Testimony at 250 [Vol. IV, Ex. 57, p. 1547] (partial list of people prepared to resign); ANGLER at 313-314 [Vol. I, Ex. 8]. The March "2004 dispute over the National Security Agency's secret surveillance program that led top Justice Department officials to threaten resignation involved computer searches through massive electronic databases, according to current and former officials briefed on the program." Opsahl Decl. Ex. 46 [Vol. IV, p. 1458] (Scott Shane & David Johnston, *Mining of Data Prompted Fight Over U.S. Spying*, N.Y. TIMES (July 29, 2007)). "[S]uch databases contain records of the phone calls and e-mail messages of millions of Americans." *Id.* Comey would later testify:

> Ultimately, the President agreed to make some changes in the Program to forestall the mass resignation. We had the president's direction to do what we believed, what the Justice Department believed was necessary to put this matter on a footing where we could certify to its legality.
>
> And so we then set out to do that. And we did that. . . . Director Mueller carried to me the president's direction that we do what the Department of Justice wanted done to put this on a sound legal footing.

Comey Testimony at 220 [Vol. IV, Ex. 57, p. 1517]; *see also* BUSH'S LAW at 184 [Vol. I, Ex. 1] (ironically, one of the changes was to rely more on the Authorization to Use Military Force justification for the Program, which later received more skepticism than the Article II argument). However, in a memo issued a few days later, the Administration also "reasserted the lawfulness of every element of the program," and asserted that the changes were "for strictly operational reasons, at the president's own discretion." ANGLER at 321 [Vol. I, Ex. 8].

As discussed more fully below, another result was that, for a period of less than 60 days, the Administration's periodic requests for cooperation from the telecommunications defendants had a giant red flag: the requests said the Program activities had been determined to be lawful by the Counsel to the President instead of the Attorney General.

B. 2007 Interactions with FISA Court

In a letter to the Congress on January 17, 2007, then Attorney General Gonzales announced that a judge of the Foreign Intelligence Surveillance Court:

> had issued orders authorizing the government to target for collection international communications where there is probable cause to believe one of the communicants is a member or agent of al Qaeda or an associated terrorist group. As a result of these orders, any electronic surveillance that was occurring as part of the Terrorist Surveillance Program will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court.

(Hepting Dkt. 127-2) [Vol. VI, Ex. 81, p. 2451] (Letter from Alberto Gonzales, Att'y Gen. of U.S., to Sen. Patrick J. Leahy, Chairman, S. Comm. on the Judiciary, and Sen. Arlen Specter, Ranking Minority Member, S. Comm. on the Judiciary (Jan. 17, 2007)). DNI McConnell later clarified that this applied to all the activities authorized in the Program Order. Sept.18, 2007, McConnell Testimony at 38-39 [Vol. II, Ex. 5, p. 812] ("All of it is subjected to the FISA court and approved by the court.")

However, the operation of the Program remained unchanged. Press Secretary Tony Snow explained on the same day "[w]hat happens is that the program pretty much continues -- the program continues." Opsahl Decl. Ex. 47, [Vol. IV, p. 1465] (White House Press Release, *Press Briefing by Tony Snow* (Jan. 17, 2007)). A reporter sought clarification:

> Q: In other words, we now have a new program called --
>
> MR. SNOW: No, you have the same program it operates under, but it's really a matter of your legal authority prior to that. It was presidential order. Now, in this case, the program continues, but it continues under the rules that have been laid out by the court.

Id. Likewise, in a background briefing given on the same day, the Administration explained that revision in the Program "wouldn't be any significant operational impact" so the Administration could "continue to do everything" under the prior Program. Opsahl Decl. Ex. 6, [Vol. I, p. 348] (Dept. of Justice Press Release, *Transcript of Background Briefing on FISA Authority of Electronic Surveillance by Senior Justice Department Officials* (Jan. 17, 2007)); *see also id.* at 351 ("the general contours under these orders allow us to do the same thing and to target the same types of communications. … the objectives of the program haven't changed and the capabilities of the intelligence agencies to operate such a program have not changed as a result of these orders"). Moreover, the basic legal rationale had not changed:

> I don't know that anything has changed. First of all, let me say that we continue to believe as we've always said and as we've explained at length that the President has the authority to authorize the terrorist surveillance program, that he has that authority under the authorization for the use of military force and under Article II of the Constitution. That's not changing.

Id.; see also Opsahl Decl. Ex. 48 [Vol. IV, p. 1469] (James Risen, *Administration Pulls Back on Surveillance Agreement*, N.Y. TIMES (May 2, 2007)) ("But on Tuesday [May 1, 2007], the senior officials, including Michael McConnell, the new director of national intelligence, said they believed that the president still had the authority under Article II of the Constitution to once again order the N.S.A. to conduct surveillance inside the country without warrants.").

"A Congressional official who has been briefed on the new procedures called it a hybrid of individual warrants and broader approval." Opsahl Decl. Ex. 49 [Vol. IV, p. 1471] (David Johnston & Scott Shane, *Senators Demand Details on New Eavesdropping Rules*, N.Y. TIMES (Jan. 19, 2007)). Rather than limit the unlawful acquisition of domestic communications, the Administration chose to focus on minimization. "At the [January 18, 2007, Senate Judiciary] hearing, Mr. Gonzales said the rules protected national security by allowing continued eavesdropping, but required the government to halt quickly the monitoring of people who were not found to be doing anything wrong." *Id; see also* Jan. 18, 2007, Gonzales Testimony at 44 [Vol. II, p. 447].

However, in May 2007, a second FISC judge refused to authorize the Program. According to the Senate Select Committee on Intelligence "[a]t the end of May 2007, however, attention was drawn to a ruling of the FISA Court. When a second judge of the FISA Court considered renewal of the January 2007 FISA orders, he issued a ruling that the DNI later described as significantly diverting NSA analysts from their counterterrorism mission to provide information to the Court." S. Rep. 110-209 (MDL Dkt. 469-2) at 5 [Vol. VIII, Ex. 90, p. 3034]. The FISC order has not been made public. *In re Motion for Release of Court Records*, 526 F.Supp.2d 484 (Foreign Intel.Surv.Ct. 2007). "One official said the issue centered on a ruling in which a FISA court judge rejected a government application for a 'basket warrant' – a term that refers to court approval for surveillance activity encompassing multiple targets, rather than warrants issued on a case-by-case basis for surveillance of specific terrorism suspects." Opsahl Decl. Ex. 50 [Vol. IV, p. 1473] (Greg Miller, *New Limits Put On Overseas Surveillance*, L.A. TIMES (Aug. 2, 2007) at A-16.)

During his August 2007 interview the *El Paso Times*, DNI McConnell said:

> [The Program] was submitted to the FISA court and the first ruling in the FISA court was what we needed to do we could do with an approval process that was at a summary level and that was OK, we stayed in business and we're doing our mission. … But the FISA process has a renewal. It comes up every so many days and there are 11 FISA judges. So the second judge looked at the same data and said well wait a minute I interpret the law, which is the FISA law, differently.

Verizon Plaintiffs' Second Supplemental Request for Judicial Notice (MDL Dkt. 363) Ex. E [Vol. VIII, Ex. 88, p. 3016] (Chris Roberts, *Transcript: Debate On The Foreign Intelligence Surveillance Act*, EL PASO TIMES (Aug. 22, 2007) at 2).

In a February 2008 interview, ODNI Spokesman Russ Feinstein clarified that "[d]ue to rulings from the FISA court, in a significant number of cases, the government had to get court orders for purely foreign-to-foreign communications that touched American wires." Opsahl Decl. Ex. 51, [Vol. IV, p. 1475] (Ryan Singel, *Can the NSA Wiretap in Iraq Without A Warrant?*, WIRED NEWS (Feb. 28, 2008)). Feinstein was correcting an earlier, and broader, statement that "if a communication touches a U.S. wire, you need a court order." *Id.*

In March 2008, Assistant Attorney General for National Security Kenneth Wainstein candidly admitted that the problem was with email communications, not phone calls. "The real concern, he said, is primarily e-mail, because 'essentially you don't know where the recipient is going to be' and so you would not know in advance whether the communication is entirely outside the United States." Opsahl Decl. Ex. 52 [Vol. IV, p. 1478] (Ellen Nakashima & Paul Kane, *Wiretap Compromise in Works: FISA Update May Hinge On Two Separate Votes*, WASH. POST (March 4, 2008) at A3); *see also* ANGLER at 455-456 [Vol. I, Ex. 8]. Accordingly, based on this evidence, it appears that the May 2007 FISC decision, at a minimum, found that the Program's bulk acquisition of email communications *prior to* the determination of whether it was foreign-to-foreign was illegal without a warrant. "[D]espite the public focus on phone calls, most of the

NSA's intercepts—75 percent by one estimate—were e-mails." BUSH'S LAW at 153 [Vol. I, Ex. 1]; *compare* Sept. 18, 2007, McConnell Testimony at 78 [Vol. II, Ex. 17, p. 811] (estimating the FISC decision effected "about two-thirds of our capability").

C. The Program After the Protect America Act of 2007

In August 2007, Congress passed the Protect America Act of 2007, Public Law 110-55 ("PAA"). In September 2007, Assistant Attorney General Wainstein wrote to Chairman Silvestre Reyes that "[t]he Protect America Act does not authorize so-called 'domestic wiretapping' without a court order, and the Executive Branch will not use it for that purpose." Opsahl Decl. Ex. 53 [Vol. IV, p. 1482] (Letter from Kenneth L. Wainstein, Asst. Att'y Gen. for Nat'l Sec., U.S. Dept. of Justice, to Rep. Silvestre Reyes, Chairman, H. Permanent Select Comm. on Intelligence (Sept.14, 2007);) *see also* Opsahl Decl. Ex. 37 [Vol. III, p. 1269] (Department of Justice Press Release, *Transcript of Conference Call with Senior Administration Officials Regarding FISA Modernization Legislation* (Aug. 7, 2007)) at 10 ("we also don't think you could direct surveillance at a large number of persons in the United States without using the FISA regime.") Accordingly, none of the assistance alleged in the various complaints was provided pursuant to the PAA.

Nevertheless, on numerous occasions, the Administration has admitted that the Program's warrantless surveillance is occurring and will continue. *See e.g.* March 2006 RJN at ¶ 3 [Vol. V, Ex. 77, p. 1773]. Despite not being authorized by the PAA, the Program continues to this day. *See* Gorman at 2 [Vol VIII, Ex. 89, p. 3024] (as of March 2008, the NSA "monitors huge volumes of records of domestic emails and Internet searches . . . "). *Newsweek* reported a few months later:

> The domestic spying measure approved by Congress last week [FISAAA] will impose new rules on government wiretapping. But it will leave largely untouched what some experts say is the most sweeping part of the secret surveillance activities ordered by President Bush after 9/11: the National Security Agency's collection of phone records and other personal data on millions of U.S. citizens. The NSA's massive "data mining" program—in which the agency's computers look for call patterns that might point to suspicious behavior—has never been publicly confirmed by the Bush administration. But industry and government officials, who asked not to be identified talking about classified matters, say the practice is a big part of what the telecoms did for the spy agency, and a key reason the companies fought so hard for the immunity from lawsuits granted by the new bill.

Opsahl Decl. Ex. 54 [Vol. IV, p. 1485] (Michael Isikoff, *Uncle Sam Is Still Watching You*, NEWSWEEK (July 21, 2008)).

As reported in *The Wall Street Journal* in March 2008, the Program still casts a wide net:

> According to current and former intelligence officials, the [NSA] now monitors huge volumes of records of domestic emails and Internet searches as well as bank transfers, credit-card transactions, travel and telephone records. The NSA receives this so-called 'transactional' data from other agencies or private companies, and its sophisticated software programs analyze the various transactions for suspicious patterns.

Gorman at 1-2 [Vol VIII, Ex. 89, p. 3023-24].

IV. Evidence Providing Context for Government Assertions on the Program

This section summarizes the evidence that provides important context for understanding the government's parsed and wordsmithed assertions about the Program that may be useful to the Court in evaluating the Mukasey Certification.

A. There is No Separate Terrorist Surveillance Program

The President and other officials have generally cabined their discussions of the Program to "the Program as described by the President," or the so-called "Terrorist Surveillance Program." *See e.g.* Mukasey Certification at 5-6; March 2006 RJN at ¶ 13 [Vol. V, Ex. 77, p. 1780-81]. Specifically, Administration officials have steered the public debate towards the portion of the Program in which the NSA intercepts communications when the agency has, in its own judgment, a "reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda," as well as the communications of individuals it deems suspicious on the basis of its belief that they have some unspecified "link" to al Qaeda or a related terrorist organization or simply "want to kill Americans." March 2006 RJN at ¶ 11 [Vol. V, Ex. 77, p. 1778-79]; *see also* Mukasey Certification at 5 (defining TSP). The officials then assert that the program as they have defined it is limited and justified. However, while the "activities acknowledged by the President after their unauthorized disclosure by *The New York Times* have been termed the Terrorist Surveillance Program ("TSP"); the TSP is not the full extent of the activities subject to periodic reauthorization." Opsahl Decl. Ex. 55 [Vol. IV, p. 1492] (Memorandum from Alberto Gonzales, Fmr. Att'y Gen. of the U.S., *Concerning the Report of Investigation Regarding Allegations of Mishandling of Classified Documents by Fmr. Att'y Gen. Alberto Gonzales* n. 8 (Aug. 28, 2008)).

A telling example of this subterfuge occurred in February 2006, when then Attorney General Gonzales testified before the Senate Judiciary Committee about the limited scope of the TSP, testifying "I've tried to outline for you and the committee what the president has authorized, *and that is all that he has authorized*." March 2006 RJN, Attachment 7 [Vol. V, Ex. 77, p. 1894] (testimony of Alberto Gonzales) at 27 (emphasis added). Later, when asked to clarify his remarks, Gonzales wrote: "I did not and could not address . . . any other classified intelligence activities . . . I was confining my remarks to [the Program] as described by the President, the legality of which was the subject. . . ." March 2006 RJN, Attachment 8 [Vol. V, Ex. 77, p. 2030] (Letter from Alberto Gonzales, Att'y Gen. of the U.S., to Sen. Arlen Specter, Chairman, S. Comm. on the Judiciary (Feb. 28, 2006)). *But see* Opsahl Decl. Ex. 56 [Vol. IV, p. 1505] (Charles Babington, *Gonzales Denies More Extensive Domestic Spying*, WASH. POST (March 3, 2006) at A04) ("Attorney General Alberto R. Gonzales told a key House Democrat yesterday that the administration is not conducting any warrantless domestic surveillance programs beyond the one that President Bush has acknowledged."). Later, Gonzales caused both confusion and accusations of perjury when he testified on July 24, 2007 that "[t]he disagreement that occurred, and the reason for the visit to the hospital, Senator, was about other intelligence activities. It was not about the terrorist surveillance program that the president announced to the American people." Opsahl Decl. Ex. 45 [Vol. IV, p. 1391] (*Oversight of the Department of Justice*: Hearing before the S. Comm. on the Judiciary, 110th Cong. (July 24, 2007)).

In a letter to Senator Arlen Specter, DNI McConnell explained:

> Shortly after 9/11, the President authorized the National Security Agency to undertake various intelligence activities … One particular aspect of these activities, and nothing more, was publicly acknowledged by the President and described in December 2005, following an unauthorized disclosure. … the Administration first used the term "Terrorist Surveillance Program" to refer specifically to that particular activity the President had publicly described in December 2005. … I understand that

> the phrase "Terrorist Surveillance Program" was not used prior to 2006 to refer to the activities authorized by the President.

Verizon RJN (MDL Dkt. 356), Ex. C [Vol. VIII, p. 3014] (Letter from J. Michael McConnell, Dir. of Nat'l Intelligence, to Sen. Arlen Specter, Ranking Member, S. Comm. on the Judiciary (July 31, 2007)).

Shortly after, then Attorney General Gonzales sent a similar letter to Senate Judiciary Committee Chair Patrick J. Leahy. Gonzales confirmed that "the President authorized the NSA to undertake a number of highly classified intelligence activities … in one executive order." *Id.* Ex. D (Letter from Alberto R. Gonzales, Att'y Gen. of U.S., to Sen. Patrick Leahy, Chairman, S. Comm. on the Judiciary (Aug. 1, 2007) at 1). Gonzales also acknowledged that "those who are knowledgeable about the NSA activities authorized in the presidential order … may be accustomed to thinking of them or referring to them together as a single NSA 'program.'" *Id.*; *see also* Opsahl Decl. Ex. 58 [Vol. IV, p. 1585] (David Johnston & Scott Shane, *Gonzales Denies Improper Pressure on Ashcroft,* N.Y. TIMES (July 25, 2007)) ("Mr. Rockefeller and Representative Jane Harman of California, who in 2004 was the top Democrat on the House Intelligence Committee, insisted that there was only one N.S.A. program, making Mr. Gonzales's assertions inaccurate. ¶ 'The program had different parts, but there was only one program,' Ms. Harman said.")[23] Likewise, Press Secretary Tony Snow explained:

> [I]n some cases, a lot of people use Terror Surveillance Program, which was a label attached to a program -- *there was never anything called the Terror Surveillance Program*. That was a label attached after the original stories appeared about the program. And it has become kind of a shorthand I think in a lot of people's minds for a whole wide swath of intelligence efforts.

Opsahl Decl. Ex. 59 [Vol. IV, p. 1590] (White House Press Release, *Press Briefing by Tony Snow* (Aug. 1, 2007)) (emphasis added).

In sum, there is no Terrorist Surveillance Program separate from surveillance under the Program, and there never was. *See also* BUSH'S LAW AT 223-224 [Vol. I, Ex. 1] ("the term itself—

[23] Rep. Harman and Sen. Rockefeller are read in to the Program. Morey Decl. Ex. S [Vol. VII, Ex. 86, p. 2768-2772] (Letter from John D. Negroponte, Dir. of Nat'l Intelligence, to J. Dennis Hastert, Speaker of the U.S. House of Representatives (May 17, 2006), at 2-3 (listing briefings that Rep. Harman and Sen. Rockefeller received about the Program).

terrorist surveillance program—did not exist just a few weeks earlier. There was no such thing. It was a creation of what would become a full-scale media blitz by the Bush White House …") We now know that the term "Terrorist Surveillance Program" is a nothing more than a marketing phrase, invented after the fact. The phrase does not describe the entire intelligence program or even an independent program, but rather only those aspects of the Program targeting al Qaeda and known affiliates. When the government has said, "the terrorist surveillance program is not a dragnet that sucks in all conversations and uses computer searches to pick out calls of interest," it means only that "one particular aspect of the Program – the portion that wiretaps terrorists – is not a dragnet." *See, e.g.,* Opsahl Decl. Ex. 60, [Vol. IV, p. 1599] (Letter from William E. Moschella, Asst. Att'y Gen., U.S. Dept. of Justice, to Sen. Arlen Specter, Chairman, S. Comm. on the Judiciary (Feb. 3, 2006) at 6). It does not mean that the government is not conducting dragnet surveillance of communications.

B. Surveillance that is Later Minimized is Still Surveillance

The government appears to exclude acquisition with subsequent minimization from its use of the word "surveillance" (despite the broader legal definition of "electronic surveillance" under applicable law).

> MR. SNOW: … the target in these conversations: a foreign individual not on U.S. soil. If that person is talking to a U.S. citizen, it does not mean that you're sitting around doing surveillance on the U.S. citizen. Furthermore, if it is a --
>
> Q But if you're surveilling a phone call, you're not just listening to the foreigner's side of the call, right?
>
> MR. SNOW: Well, yes, but on the other hand, if -- you probably understand that if somebody is just calling in and asking how his socks are at the dry cleaners, all of that personal information is combed out and, in fact, the U.S. citizen basically – you're not conducting surveillance.

Opsahl Decl. Ex. 61 [Vol. IV, p. 1606] (White House Press Release, *Press Briefing by Tony Snow* (Aug. 8, 2007)). The Administration's definition of surveillance, however, ignores how the Program initially acquires the entirety of communications, meaning that the telecommunications carrier defendants' role is complete before minimization.

Likewise, the NSA takes the position that " 'acquisition' of content does not take place until a conversation is intercepted and processed 'into an intelligible form intended for human inspection.'" Cohn Decl. Ex. F [Vol. V, Ex. 76, p. 1750] (Barton Gellman, et al., *Surveillance Net Yields Few Suspects: NSA's Hunt for Terrorists Scrutinizes Thousands of Americans, but Most Are Later Cleared*, WASH. POST (Feb. 5, 2006) at A01.) By narrowly defining words like acquisition and surveillance, the Administration can make sweeping claims that give a deceptive impression.

C. Misleading Use of the Terms "Content," "Communications" and "Conversations"

The government's word games are best illustrated by then Principal Deputy Director of National Intelligence Hayden's appearance before the National Press Club in January 2006. It was just after the Program came to light, and Hayden, as the former Director of the NSA, attempted to downplay fears. Hayden said:

> Let me talk for a few minutes also about what this program is not. It is not a driftnet over Dearborn or Lackawanna or Freemont grabbing conversations that we then sort out by these alleged keyword searches or data-mining tools or other devices that so-called experts keep talking about.

March 2006 RJN, Attachment 4 [Vol. V, Ex. 77, p. 1802] (Michael Hayden, *Remarks at the National Press Club on NSA Domestic Surveillance* (Jan. 23, 2006)); *see also* Opsahl Decl. Ex. 62, [Vol. IV, p. 1614] (Letter from William E. Moschella, Asst. Att'y Gen., U.S. Dept. of Justice, to Sen. Arlen Specter, Chairman, S. Comm. on the Judiciary (Mar. 24, 2006) at 4 (response to Senator Leahy's question 7 employs same misdirection)).

Later, however, after the May 11, 2006 *USA Today* story brought the government's access to a vast database of domestic calls to the attention of the American public, Hayden had to explain. During his confirmation hearing later that month, Hayden backtracked, testifying:

> [A]t key points, key points in my remarks, I pointedly and consciously downshifted the language I was using.
>
> When I was talking about a drift net over Lackawanna or Freemont or other cities, I switched from the word "communications" to the much more specific and unarguably accurate conversation.

Hayden Hearing at 50 [Vol. I, Ex. 2, p. 53]; *compare* Gorman at 5-6 [Vol VIII, Ex. 89, p. 3026-27] (quoting Hayden's National Press Club appearance and then noting that "intelligence officials now say the broader NSA effort amounts to a driftnet."); ANGLER at 149 [Vol. I, Ex. 8] ("In other words, there was a drift net over America. … The drift net collected the so-called metadata of domestic communications—the web links we clicked, the numeric addresses of our computers, the 'to' and 'from' and 'subject lines' of our emails, the telephone numbers we dialed, the parties and times and durations of our calls.").

With respect to making use of the content of the communications, Hayden later testified that the NSA would listen to conversations if "we had reason to believe that that communication, one or both of those communicants were associated with al Qaeda." Hayden Hearing at 50-51 [Vol. I, Ex. 2, p. 53-54]. Hayden testified that "we do not use the content of communications to decide which communications we want to study the content of." *Id.* at 50 [Vol. I, Ex. 2, p. 53]. However, Hayden's next words show he was using a crabbed definition of "content" that excludes the subject lines of email and the URLs of web links: "in other words, when we look at the content of the communications, everything between 'hello' and 'good bye'…." *Id.*

This is another variation on the word game, since the legal definition of "contents" includes email subject lines and URLs. *See* 18 U.S.C. § 2510(8) and 50 U.S.C. § 1801(n). The government has, in other contexts, admitted that meta-data like the "subject lines" of email and the URLs of web links are the "content of communications." *See* Opsahl Decl. Ex. 64 [Vol. IV, p. 1631] (Computer Crime and Intellectual Property Section, U.S. Dept. of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations,* Chapter 3 (2002)) ("[t]he subject headers of e-mails are also contents."); Opsahl Decl. Ex. 64 [Vol. IV, p. 1631] (U.S Dept. of Justice, *U.S. Attorneys' Manual* 9-7.500 (2003)) (prohibiting the collection of URLs without prior consultation with DOJ to determine whether the URLs to be collected will constitute content or not.).

Likewise, DNI McConnell has used the word "content" to exclude meta-data in the same extra-legal fashion:

> Mr. HOLT. Do you need to be able to conduct bulk collection of call detail records, metadata for domestic-to-domestic phone calls by Americans?

> Director MCCONNELL. *Metadata, we think of it as not content* but a process for how you would find something you might be looking for. Think of it as a roadmap.

September 20, 2007, McConnell Testimony at 80 [Vol. VIII, Ex. 92, p. 3209].

D. The Government's Assertions of Harm to National Security Are Not Credible

Throughout this litigation the government has asserted that the revelation of certain information "would cause exceptionally grave harm to the national security." *See, e.g.,* Mukasey Certification at 5-7. However, the record is replete with instances in which the government later publicly disclosed the very same information.

For example, on May 24, 2007, the government asserted that "Plaintiffs in these cases put directly at issue whether or not the NSA has conducted particular intelligence activities and whether or not it has done so *with the secret help of a private entity*. The disclosure of any information that would tend to confirm or deny these allegations … would cause exceptionally grave harm to the national security." May 24, 2007, Public Declaration of Michel McConnell (MDL Dkt. 254) at ¶ 16 [Vol. VI, Ex. 85, p. 2552] (emphasis added).

Likewise, the government's August 7, 2007 response to the *Hepting* plaintiffs' Ninth Circuit request for judicial notice of Attorney General Gonzales' July 24, 2007, testimony stated that revealing even the "type of company" who assisted the government would result in "potentially grave harm to national security." Opsahl Decl. Ex. 65 [Vol. IV, p. 1651-52] (Government's Response to Plaintiffs' Request for Judicial Notice at 5-6).

Nevertheless, the government later freely disclosed both that the private sector helped and that the providers were telecommunications companies, especially in the context of the push for passage of Section 802. *See* Section II, *supra*, *citing* September 20, 2007, McConnell Testimony at 11 [Vol. VIII, p. 3140]; Opsahl Decl. Ex. 96 [Vol. VIII, p. 3244] (White House Press Release, *Straight To The Point* (Feb. 28, 2008)); Opsahl Decl. Ex. 95, [Vol. VIII, p. 3242]; (White House Press Release, *Statement by the Press Secretary on FISA* (Feb. 25, 2008) at 1); *Id.* Ex. 32 [Vol. III, p. 1192] (Feb. 12, 2008 *Press Briefing by Dana Perino* at 4); *Id.* Ex. 15 [Vol. II, p. 720-27] (White House Press Release, *Transcript of Background Briefing by Senior Administration Officials on*

FISA (Feb. 26, 2008)); and *Id.* Ex. 29 [Vol. III, p. 1176]. (Oct. 31, 2007, S. Judiciary Comm. Hearing).

Likewise, in DNI McConnell's May 25, 2007, declaration in *Shubert v. Bush*, the government asserted that "grave danger" would result from the disclosure of "[i]nformation that may tend to *confirm or deny* whether Verizon/MCI, AT&T, or any other telecommunications carrier has assisted the NSA with the alleged intelligence activities." May 25, 2007, Public Declaration of J. Michael McConnell (MDL Dkt. 295) ¶¶ 11c, 13 (emphasis added) [Vol. IV, Ex. 85, p. 2550]; However, the Attorney General's recent certification denies that Verizon/MCI, AT&T, or any other telecommunications carrier has assisted the NSA with the alleged content dragnet. Mukasey Certification at 5

In moving to dismiss the Verizon plaintiffs' case, the government argued "Plaintiffs' content surveillance claim in this case (as in *Hepting*) boils down to an unfounded and highly speculative allegation that they do not believe that the President authorized only a limited surveillance program directed at certain al Qaeda-related international communications." Memo of P&A in support of Motion to Dismiss the Verizon Master Consolidated Complaint (MDL Dkt. 254) at 3 [Vol. VI, Ex. 84, p. 2470]. Proving whether or not the President authorized more, the government asserted, would cause "grave danger." *Id.* (citing May 25, 2007, Public Declaration of J. Michael McConnell (MDL Dkt. 295)).

Nevertheless, on July 31, 2007, DNI McConnell admitted that the President authorized more than a limited surveillance program directed at certain al Qaeda-related international communications. Verizon RJN (MDL Dkt. 356), Ex. C (Letter from J. Michael McConnell, Dir. of Nat'l Intelligence, to Sen. Arlen Specter, Ranking Member, S. Comm. on the Judiciary (July 31, 2007)); *see also Id.* Ex. D (Letter from Alberto R. Gonzales, Att'y Gen. of U.S., to Sen. Patrick Leahy, Chairman, S. Comm. on the Judiciary (Aug. 1, 2007) at 1 ("the President authorized the NSA to undertake a number of highly classified intelligence activities … in one executive order.")).

The *Al-Haramin* plaintiffs also brought to the Court's attention another example, comparing a statement by FBI Deputy Director John Pistole that contradicted government's prior assertion that whether or not the *Al-Haramain* plaintiffs were surveillance could not be disclosed. Al-Haramain Motion Pursuant to § 1806(f) (MDL Dkt. 472) at 6-7 [Vol. VIII, p. 3112-13].

V. Evidence of Attorney General Mukasey's Bias on Telecom Immunity

A. Evidence of the Attorney General's Institutional Responsibilities That Provide A Strong Motive To Rule In A Way That Would Aid The Institution

The Attorney General's client strongly supports immunity. *See, e.g.,* Opsahl Decl. Ex. 66, [Vol. IV, p. 1662] (Executive Office of the President, Statement of Administration Policy S. 2248 (Dec. 17, 2007)) ("It is imperative that Congress provide liability protection to those who cooperated with this country in its hour of need.") Likewise, Vice President Cheney emphasized the Administration's position: "One might even suppose that without liability protection for past activities to aid the government, the private sector might be extremely reluctant to comply with future requests from the government … That risk is unacceptable to the President." Opsahl Decl. Ex. 67, [Vol. IV, p. 1666] (Richard Cheney, Vice Pres. of the U.S., *Vice President's Remarks to the Heritage Foundation* (Jan. 23, 2008)).

On February 28, 2008, President Bush explained the institutional issues that he believed required immunity, saying: "Allowing these lawsuits to proceed could make it harder to track the terrorists, because private companies besieged by and fearful of lawsuits would be less willing to help us quickly get the information we need." Opsahl Decl. Ex. 68 [Vol. IV, p. 1668] (White House Press Release, *Press Conference of the President* (Feb. 28, 2008)). He also said, "You cannot expect phone companies to participate if they feel like they're going to be sued." *Id.*

In addition, the Department of Justice has its own institutional interest in immunity. In a February 26, 2008 press conference, a Senior Administration Official explained the DOJ's institutional concerns. Opsahl Decl. Ex. 15 [Vol. II, p. 724] (*Transcript of Background Briefing by Senior Administration Officials on FISA* (Feb. 26, 2008) ("Keep in mind who we're up representing. I'm in the Department of Justice.")). First, the Administration noted that the impetus for action on immunity was the plaintiffs' success in this Multi-District Litigation. *Id.* at 4 [Vol. II, p. 723] (the "bottom line is that some of these cases have gotten some traction."). Next, the Administration explained the institutional interests: "we have an interest in this [because] we rely on the providers to cooperate. We don't own the communication systems. We have to work with them." *Id.* This cooperation, the Administration asserted, was threatened: "because there's no immunity, the providers are understandably concerned. They've got shareholders, they've got fiduciary duties to their shareholders, they've got to protect them." *Id.* at 5 [Vol. II, p. 724].

> So these general counsels are doing their jobs. They're saying, wait a minute, is that potential liability? We've got billions of dollars in liability looming in the background here from -- that we haven't been immunized from. We're very worried about that. We're not seeing immunity coming down the road any time real soon. …
>
> It was a back-and-forth engagement with the general counsels' offices, so that they got to the point where, as the announcement says, they were willing to comply with our requests, but there's no guarantee they'd continue to do so.

Id.

> However, they've made it very clear that this isn't a permanent situation, and they're concerned about it and they might -- they may well withdraw that cooperation if the situation doesn't get cleared up with permanent legislation.

Id. The evidence shows that the Attorney General and his client has a strong intuitional interest in obtaining immunity for the defendants in these lawsuits.

B. Evidence that the Attorney General Has Prejudged This Matter

Over the last year, Attorney General Mukasey has made numerous statements that illustrate that he has pre-judged the question of whether the defendants should get immunity from these lawsuits. In November 2007, the Attorney General wrote to Senator Leahy, Chairman of the Senate Judiciary Committee:

> Congressional action to provide protection from private lawsuits against companies that are alleged to have assisted the Government in the aftermath of the September 11th terrorist attacks on America also is critical to ensuring the Government can continue to receive private sector help to protect the Nation.

Opsahl Decl. Ex. 69 [Vol. IV, p. 1676] (Letter from Michael Mukasey, Att'y Gen. of the U.S., and J. Michael McConnell, Dir. of Nat'l Intelligence, to Sen. Patrick Leahy, Chairman, S. Comm. on the Judiciary (Nov. 14, 2007)).

In December 2007, the Attorney General wrote an op-ed for *USA Today*, calling the proposed legislative immunity provisions "critical," and opined that "[w]e cannot expect, nor do we want, companies to second-guess the government's determination of the necessity and lawfulness of requested assistance." Opsahl Decl. Ex. 70 [Vol. IV, p. 1681] (Michael Mukasey, Att'y Gen. of the U.S., Op-Ed., *We Balance Security, Privacy: Immunity For Telecoms Is Critical To Efforts To Protect The Nation*, USA TODAY (Dec. 20, 2007) at A12); *see also* Opsahl Decl. Ex. 71 [Vol. IV, p. 1683] (Michael Mukasey, Att'y Gen. of the U.S., Op-Ed., *A FISA Fix*, L.A. TIMES (Dec. 12, 2007) at A31) ("It is unfair to force such companies to face the possibility of massive judgments and litigation costs"); Opsahl Decl. Ex. 72 [Vol. IV, p. 1685] (Michael Mukasey, Att'y Gen. of the U.S., *Prepared Remarks of Attorney General Michael B. Mukasey at the American Bar Association National Security Law Breakfast* (Dec. 19, 2007) ("immunity [is] a fair and just result. … it makes no sense to allow this litigation to go forward.")).

In February 2008, Attorney General Mukasey wrote to Rep. Reyes, Chairman of the House Permanent Select Committee on Intelligence, that "providing liability protection to those companies sued for answering their country's call for assistance in the aftermath of September 11 is *simply the right thing to do*." Opsahl Decl. Ex. 73, [Vol. IV, p. 1690] (Letter from Michael Mukasey, Att'y Gen. of the U.S., and J. Michael McConnell, Dir. of Nat'l Intelligence, to Rep. Silvestre Reyes, Chairman, H. Permanent Select Comm. on Intelligence (Feb. 22, 2008)) (emphasis added).

Similarly, in June 2008, the Attorney General and DNI McConnell wrote a letter to Senate Majority Leader Reid opposing certain proposed amendments to the FISAAA that ultimately were not enacted. The Attorney General opined that "[a]ffording liability protections to those companies believed to have assisted the Government with communications intelligence activities in the aftermath of September 11th is a just result… ." Opsahl Decl. Ex. 74, [Vol. IV, p. 1694] (Letter from Michael Mukasey, Att'y Gen. of the U.S., and J. Michael McConnell, Dir. of Nat'l Intelligence, to Sen. Harry Reid, S. Majority Leader (June 26, 2008)). The Attorney General stated that allowing this Court to rule on the constitutionality of the Administration's arguments for warrantless wiretapping "is unacceptable." *Id.* The Attorney General argued that "the aim of the amendment appears to be an adjudication of the Government's prior actions," and that "by requiring a merits adjudication of the plaintiffs' constitutional claims" the proposed amendment "would significantly negate a major purpose of the retroactive liability protections." *Id.*

In July 2008, the Attorney General opined in another letter to Senator Reid that "[l]iability protection is the fair and just result and is necessary to ensure the continued assistance of the private sector." Opsahl Decl. Ex. 75 [Vol. IV, p. 1697] (Letter from Michael Mukasey, Att'y Gen. of the U.S., and J. Michael McConnell, Dir. of Nat'l Intelligence, to Sen. Harry Reid, S. Majority Leader (July 7, 2008)). The Attorney General also decried an amendment that would have postponed implementation of retroactive immunity until after the Inspector General files a report on the spying program, contending that "the apparent purpose of the amendment is to postpone a decision on whether to provide liability protection at all. Such a result would *defeat the point* of the carefully considered and bipartisan retroactive liability protections." *Id.* (emphasis added).

CONCLUSION

The plaintiffs respectfully request that the Court consider this Summary of Voluminous Evidence pursuant to Rule 1006, including evidence previously submitted and the new evidence submitted with the accompanying Declaration of Kurt Opsahl, in its assessment of whether the government has met its burden of presenting substantial evidence in support of the Mukasey Certification submitted as part of the United States' Section 802 Motion. This summary is offered to aid the Court in determining a critical issue by bringing together a summary of plaintiffs' relevant evidence that the Court may consider at this stage of the litigation.

DATED: October 16, 2008

Respectfully submitted,

/s/ Kurt Opsahl

ELECTRONIC FRONTIER FOUNDATION
Cindy A. Cohn, Esq. (SBN 145997)
Lee Tien, Esq. (SBN 148216)
Kurt Opsahl, Esq. (SBN 191303)
Kevin S. Bankston, Esq. (SBN 217026)
Corynne McSherry, Esq. (SBN 221504)
James S. Tyre, Esq. (SBN 83117)
454 Shotwell Street
San Francisco, CA 94110

ROGER BALDWIN FOUNDATION OF ACLU
Harvey Grossman
Adam Schwartz
180 North Michigan Avenue
Suite 2300
Chicago, IL 60601
Telephone: (312) 201-9740
Facsimile: (312) 201-9760

COUNSEL FOR
AT&T CLASS PLAINTIFFS AND
CO-CHAIR OF PLAINTIFFS' EXECUTIVE
COMMITTEE

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN
CALIFORNIA
Ann Brick (SBN 65296)
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493
Facsimile: (415) 255-8437
COUNSEL FOR PLAINTIFFS IN
CAMPBELL v. AT&T AND RIORDAN v.
VERIZON COMMUNICATIONS INC.

FENWICK & WEST LLP
Laurence F. Pulgram (SBN 115163)
Jennifer Kelly (SBN 193416)
Candace Morey (SBN 233081)
555 California Street, 12th Floor
San Francisco, CA 94104
Telephone: (415) 875-2300
Facsimile: (415) 281-1350
COUNSEL FOR PLAINTIFFS IN
CAMPBELL v. AT&T AND RIORDAN v.
VERIZON COMMUNICATIONS INC.

MOTLEY RICE LLC
Ronald Motley
Donald Migliori
Jodi Westbrook Flowers
Vincent I. Parrett
28 Bridgeside Boulevard
P.O. Box 1792
Mt. Pleasant, SC 29465
Telephone: (843) 216-9000
Facsimile: (843) 216-9450
PLAINTIFFS' COUNSEL FOR VERIZON
SUBSCRIBER CLASS

THE MASON LAW FIRM, PC
Gary E. Mason
Nicholas A. Migliaccio
1225 19th St., NW, Ste. 500
Washington, DC 20036
Telephone: (202) 429-2290
Facsimile: (202) 429-2294

Telephone: (415) 436-9333 x108
Facsimile: (415) 436-9993
COUNSEL FOR
AT&T CLASS PLAINTIFFS AND
CO-CHAIR OF PLAINTIFFS' EXECUTIVE
COMMITTEE

LAW OFFICE OF RICHARD R. WIEBE
Richard R. Wiebe (SBN 121156)
425 California Street
Suite 2025
San Francisco, CA 94104
Telephone: (415) 433-3200
Facsimile: (415) 433-6382
COUNSEL FOR AT&T CLASS PLAINTIFFS

LIEFF, CABRASER, HEIMANN &
BERNSTEIN, LLP
Elizabeth J. Cabraser
Barry R. Himmelstein
Eric B. Fastiff
275 Battery Street, 30th Floor
San Francisco, CA 94111-3339
Telephone: (415) 956-1000
Facsimile: (415) 956-1008
PLAINTIFFS' COUNSEL FOR MCI
SUBSCRIBER CLASS

GEORGE & BROTHERS, L.L.P.
R. James George, Jr.
Douglas Brothers
1100 Norwood Tower
114 W. 7th Street
Austin, Texas 78701
Telephone: (512) 495-1400
Facsimile: (512) 499-0094
PLAINTIFFS' COUNSEL FOR CINGULAR
SUBSCRIBER CLASS

LISKA, EXNICIOS & NUNGESSER
ATTORNEYS-AT-LAW
VAL PATRICK EXNICIOS
One Canal Place, Suite 2290
365 Canal Street
New Orleans, LA 70130
Telephone: (504) 410-9611

PLAINTIFFS' COUNSEL FOR SPRINT SUBSCRIBER CLASS

Facsimile: (504) 410-9937
PLAINTIFFS' COUNSEL FOR BELLSOUTH SUBSCRIBER CLASS

BRUCE I AFRAN, ESQ.
10 Braeburn Drive
Princeton, NJ 08540
609-924-2075
PLAINTIFFS' COUNSEL FOR BELLSOUTH SUBSCRIBER CLASS

KRISLOV & ASSOCIATES, LTD.
CLINTON A. KRISLOV
20 North Wacker Drive
Suite 1350
Chicago, IL 60606
Telephone: (312) 606-0500
Facsimile: (312) 606-0207
PLAINTIFFS' COUNSEL FOR BELLSOUTH SUBSCRIBER CLASS

MAYER LAW GROUP LLC
CARL J. MAYER
66 Witherspoon Street, Suite 414
Princeton, New Jersey 08542
Telephone: (609) 921-8025
Facsimile: (609) 921-6964
PLAINTIFFS' COUNSEL FOR BELLSOUTH SUBSCRIBER CLASS

THE LAW OFFICES OF STEVEN E. SCHWARZ, ESQ.
STEVEN E. SCHWARZ
2461 W. Foster Ave., #1W
Chicago, IL 60625
Telephone: (773) 837-6134
PLAINTIFFS' COUNSEL FOR BELLSOUTH SUBSCRIBER CLASS